

English translation of the original article:

Les θ -régulateurs locaux d'un nombre algébrique – Conjectures p -adiques

Canadian Journal of Mathematics, Vol. **68**, 3 (2016), 571–624

LOCAL θ -REGULATORS OF AN ALGEBRAIC NUMBER p -ADIC CONJECTURES

GEORGES GRAS

ABSTRACT. Let K/\mathbb{Q} be Galois and let $\eta \in K^\times$ be such that the multiplicative $\mathbb{Z}[G]$ -module generated by η is of \mathbb{Z} -rank n . We define the local θ -regulators $\Delta_p^\theta(\eta) \in \mathbb{F}_p$ for the \mathbb{Q}_p -irreducible characters θ of $G = \text{Gal}(K/\mathbb{Q})$. Let V_θ be the θ -irreducible representation. A linear representation $\mathcal{L}^\theta \simeq \delta V_\theta$ is associated with $\Delta_p^\theta(\eta)$ whose nullity is equivalent to $\delta \geq 1$ (Theorem 3.9). Each $\Delta_p^\theta(\eta)$ yields $\text{Reg}_p^\theta(\eta)$ modulo p in the factorization $\prod_\theta (\text{Reg}_p^\theta(\eta))^{\varphi(1)}$ of $\text{Reg}_p^G(\eta) := \frac{\text{Reg}_p(\eta)}{p^{[K:\mathbb{Q}]}}$ (normalized p -adic regulator of η), where $\varphi \mid \theta$ is absolutely irreducible. From the probability $\text{Prob}(\Delta_p^\theta(\eta) = 0 \ \& \ \mathcal{L}^\theta \simeq \delta V_\theta) \leq p^{-f\delta^2}$ (f = residue degree of p in the field of values of φ) and the Borel–Cantelli heuristic, we conjecture that, for p large enough, $\text{Reg}_p^G(\eta)$ is a p -adic unit or that $p^{\varphi(1)} \parallel \text{Reg}_p^G(\eta)$ (existence of a single θ of G with $f = \delta = 1$ and no extra p -divisibility); this obstruction may be lifted assuming the existence of a binomial probability law (Sec. 7) confirmed through numerical studies (with groups $G = C_3, C_5, D_6$). This conjecture would imply that, *for all p large enough*, Fermat quotients of rationals and normalized p -adic regulators are p -adic units (Theorem. 1.1), whence the fact that number fields are p -rational for $p \gg 0$. We recall §8.7 some deep cohomological results, which may strengthen such conjectures.

1. INTRODUCTION

Let K/\mathbb{Q} be a Galois extension of degree n of Galois group G . Let $\eta \in K^\times$. An exponential notation is used for conjugation of η by $\sigma \in G$, which implies the writing $(\eta^\sigma)^\tau =: \eta^{\tau\sigma}$ for all $\sigma, \tau \in G$ (law of left G -module). We assume that the multiplicative $\mathbb{Z}[G]$ -module generated by η is of \mathbb{Z} -rank n (i.e., $\langle \eta \rangle_G \otimes \mathbb{Q} \simeq \mathbb{Q}[G]$). For p large enough, we put $\text{Reg}_p^G(\eta) := \det\left(\frac{-1}{p} \log_p(\eta^{\tau\sigma^{-1}})\right)_{\sigma, \tau \in G}$ (normalized p -adic regulator of η).

We shall see that the unique obstruction, to apply the heuristic principle of Borel–Cantelli leading (conjecturally) to a finite number of p such that $\text{Reg}_p^G(\eta) \equiv 0 \pmod{p}$, is related to primes p such that $\text{Reg}_p^G(\eta)$ is exactly divisible by a minimal power of p ; this is equivalent to $\text{Reg}_p^G(\eta) \sim p^{\varphi(1)}$ (equality up to a p -adic unit), where the character φ (absolutely irreducible) defines a p -adic character θ satisfying certain conditions (Definition 4.1).

Date: January 7, 2017.

1991 *Mathematics Subject Classification.* Primary 11F85; Secondary 11R04; 20C15; 11C20; 11R37; 11R27; 11Y40.

Key words and phrases. p -adic regulators; Frobenius group determinants; p -adic characters; Leopoldt–Jaulent conjecture; Abelian p -ramification; p -rationality; Fermat quotient; probabilistic number theory.

Such a situation is a priori of probability at most $\frac{O(1)}{p}$, only when η is considered as a random variable; it is the unique case where the Borel–Cantelli principle does not apply (see Section 9 for some enlightenment). We intend, from heuristics and numerical experiments, to remove this obstruction and to reach the following probabilistic result, *when η is fixed and $p \rightarrow \infty$* :

Theorem 1.1. *Let K/\mathbb{Q} be a Galois extension of degree n and of Galois group G . Let $\eta \in K^\times$ be fixed, η generating a multiplicative $\mathbb{Z}[G]$ -module of \mathbb{Z} -rank n .*

- (i) *Under the Heuristic 7.4 (existence of a classical binomial law of probability), the probability to have $\text{Reg}_p^G(\eta) \equiv 0 \pmod{p}$ is at most $\frac{C_\infty(\eta)}{p^{\log_2(p)/\log(c_0(\eta)) - O(1)}}$ for $p \rightarrow \infty$, where $c_0(\eta) = \max_{\sigma \in G}(|\eta^\sigma|)$, $e^{-1} \leq C_\infty(\eta) \leq 1$, and $\log_2 = \log \circ \log$.*
- (ii) *Under the previous heuristic 7.4 and the principle of Borel–Cantelli, the number of primes p such that $\text{Reg}_p^G(\eta) \equiv 0 \pmod{p}$ is finite.*

We shall always suppose that the prime number p that we consider is large enough, in particular odd, not divisor of n , unramified in K , and prime to η , so that the normalized p -adic regulator $\text{Reg}_p^G(\eta) := p^{-[K:\mathbb{Q}]} \cdot \text{Reg}_p(\eta)$ makes sense in \mathbb{Z}_p , where $\text{Reg}_p(\eta)$ is the usual p -adic regulator of η (see § 2.1.3).

Denote by Z_K (resp. $Z_{K,(p)}$) the ring of integers (resp. of p -integers) of K ; for $K = \mathbb{Q}$, one gets \mathbb{Z} (resp. $\mathbb{Z}_{(p)}$). For all place $v \mid p$ of K , we denote by $\mathfrak{p}_v \mid p$ the prime ideal associated with v .

If n_p is the common residue degree of the places $v \mid p$ in K/\mathbb{Q} , the multiplicative groups of the residue fields are of order $p^{n_p} - 1$ and for all $v \mid p$ we have the congruence $\eta^{p^{n_p}-1} \equiv 1 \pmod{\mathfrak{p}_v}$; hence finally, since $\prod_{\mathfrak{p}_v \mid p} \mathfrak{p}_v = p Z_K$,

$$\eta^{p^{n_p}-1} = 1 + p \alpha_p(\eta), \quad \alpha_p(\eta) \in Z_{K,(p)},$$

which leads, by Galois, to the relations

$$\alpha_p(\eta^\sigma) = \alpha_p(\eta)^\sigma \text{ for all } \sigma \in G,$$

and to the “logarithmic” properties

$$\alpha_p(\eta \eta') \equiv \alpha_p(\eta) + \alpha_p(\eta') \pmod{p Z_{K,(p)}} \quad \& \quad \alpha_p(\eta^\lambda) \equiv \lambda \alpha_p(\eta) \pmod{p Z_{K,(p)}}$$

(for $\eta, \eta' \in K^\times$, $\lambda \in \mathbb{Z}$).

This *generalized Fermat quotient* $\alpha_p(\eta)$ of η is the key element of our study. More precisely, the properties of the G -module generated by $\alpha_p(\eta)$ modulo $p Z_{K,(p)}$ shall precise the properties of the *normalized p -adic regulators* of η , in particular for the search of the (rares) solutions p giving their divisibility by p . The numerical illustrations are obtained by means of PARI programs (from [P]).

2. REGULATORS AND REPRESENTATIONS – LOCAL REGULATORS

2.1. p -adic logarithm – p -adic regulators. Let p be a fixed prime number satisfying the hypothesis given in the Introduction. We suppose that the number field K is considered as a subfield of \mathbb{C}_p . Thus, any “embedding” of K into \mathbb{C}_p is nothing else than a \mathbb{Q} -automorphism $\sigma \in G$.

Let $\mathfrak{p}_0 = \mathfrak{p}_{v_0}$ be a prime ideal of K above p and let $D_{\mathfrak{p}_0}$ be its decomposition group. The places $v \mid p$, conjugates of v_0 , correspond to the $(G : D_{\mathfrak{p}_0})$ distinct prime ideals $\mathfrak{p}_v := \mathfrak{p}_0^{\sigma_v}$, where $(\sigma_v)_{v \mid p}$ is an exact system of representatives of $G/D_{\mathfrak{p}_0}$.

We consider the $\mathbb{Q}_p[G]$ -module $\prod_{v|p} K_v$ where $K_v = \sigma_v(K) \mathbb{Q}_p \subset \mathbb{C}_p$, is the completion of K at v ; as K/\mathbb{Q} is Galois, K_v/\mathbb{Q}_p is independent of $v|p$ but the notation K_v recalls that this local extension is *provided* with the embedding $\sigma_v : K \rightarrow K_v \subset \mathbb{C}_p$, which allows the diagonal embedding with dense image

$$i_p := (\sigma_v)_{v|p} : K \longrightarrow \prod_{v|p} K_v$$

where $i_p(x) := (\sigma_v(x))_{v|p}$, and which implies that $K \otimes \mathbb{Q}_p \simeq \prod_{v|p} K_v \simeq \mathbb{Q}_p[G]$ (semi-local theory). By abuse, if $x \in K$, we shall write $x \in \prod_{v|p} K_v$, i_p being understood.

2.1.1. p -adic logarithm on K^\times . The p -adic logarithm $\log_p : K^\times \rightarrow K \otimes \mathbb{Q}_p$ is defined on the set $\{1 + px, x \in Z_{K,(p)}\}$, by means of the usual series ($p > 2$)

$$\log_p(1 + px) = \sum_{i \geq 1} (-1)^{i+1} \frac{(px)^i}{i} \equiv px \pmod{p^2},$$

noting that $\sum_{i=1}^N (-1)^{i+1} \frac{(px)^i}{i} \in K$ for any $N \geq 1$. In the case of $\gamma \in K_{(p)}^\times$, we use the functional relation

$$\log_p(\gamma) = \frac{1}{p^{n_p} - 1} \log_p(\gamma^{p^{n_p} - 1}) = \frac{1}{p^{n_p} - 1} \log_p(1 + p \alpha_p(\gamma)) \equiv -p \alpha_p(\gamma) \pmod{p^2}.$$

More generally, this \log_p function, seen modulo p^{N+1} , $N \geq 1$, is represented by elements of $Z_{K,(p)}$ and is an homomorphism of G -modules for the law defined, for all $\sigma \in G$, by $\sigma(\log_p(\gamma) \pmod{p^{N+1}}) := \log_p(\gamma^\sigma) \pmod{p^{N+1}}$, using the congruence (where N' is an obvious function of N)

$$\sigma(\log_p(\gamma) \pmod{p^{N+1}}) \equiv \frac{1}{p^{n_p} - 1} \sum_{1 \leq i \leq N'} (-1)^{i+1} \frac{(p \alpha_p(\gamma)^\sigma)^i}{i} \pmod{p^{N+1}},$$

defining an element of $Z_{K,(p)}$ which approximates $\log_p(\gamma^\sigma)$ modulo p^{N+1} . So $\sigma_v(\log_p(\gamma))$ makes sense in K_v for all $v|p$.

2.1.2. p -adic rank. Let $\text{Log}_p := \log_p \circ i_p = (\sigma_v)_{v|p} \circ \log_p$ be the homomorphism of G -modules defined, on the subgroup of elements of K^\times prime to p , by

$$\text{Log}_p(\gamma) = (\log_p(\gamma^{\sigma_v}))_{v|p} \in \prod_{v|p} K_v.$$

Let $\eta \in K^\times$, prime to p , and let F be the $\mathbb{Z}[G]$ -module generated by η . We call p -adic rank of F , the integer

$$\text{rg}_p(F) := \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \text{Log}_p(F)).$$

The use of Log_p is a commodity since by conjugation by the elements of G , the knowledge of \log_p implies that of Log_p and conversely by projections $\prod_{v'|p} K_{v'} \rightarrow K_v$. To make a link with the concept of p -adic regulator, we shall prove first the following two technical results:

Lemma 2.1. *Let p be an odd prime, unramified in K , and let $\lambda \in Z_{K,(p)}$. If $\lambda \notin p Z_{K,(p)}$, there exists $u \in K^\times$, prime to p , such that $\text{Tr}_{K/\mathbb{Q}}(\lambda u) \not\equiv 0 \pmod{p}$.*

Proof. For all $u \in K^\times$, prime to p , consider the diagonal embedding of λu in $\prod_{v|p} K_v$, and let Tr_v be the local traces $\text{Tr}_{K_v/\mathbb{Q}_p}$ for $v|p$. Then

$$\text{Tr}_{K/\mathbb{Q}}(\lambda u) = \sum_{v|p} \text{Tr}_v(\sigma_v(\lambda u)).$$

By assumption, there exists a non-empty set Σ of places $v \mid p$ such that $\sigma_v(\lambda)$ (hence $\sigma_v(\lambda u) = \sigma_v(\lambda) \sigma_v(u)$ for all u prime to p) is a unit of K_v .

For $v_1 \in \Sigma$, write

$$\mathrm{Tr}_{K/\mathbb{Q}}(\lambda u) = \sum_{v \mid p, v \neq v_1} \mathrm{Tr}_v(\sigma_v(\lambda u)) + \mathrm{Tr}_{v_1}(\sigma_{v_1}(\lambda u)) =: a + \mathrm{Tr}_{v_1}(\sigma_{v_1}(\lambda u)).$$

As p is unramified in K , the residue traces at p are surjective and since $\sigma_{v_1}(\lambda u)$ is a unit, it is sufficient to take a suitable $u \equiv 1 \pmod{\prod_{v, v \neq v_1} \mathfrak{p}_v}$ (in which case $a \in \mathbb{Z}_p \pmod{p}$ does not depend on u) and $u \equiv u_1 \pmod{\mathfrak{p}_{v_1}}$ such that for instance $\mathrm{Tr}_{v_1}(\sigma_{v_1}(\lambda u)) \equiv 1 - a \pmod{p}$ if $a \not\equiv 1 \pmod{p}$ (resp. $1 \pmod{p}$ if $a \equiv 1 \pmod{p}$). Whence $\mathrm{Tr}_{K/\mathbb{Q}}(\lambda u) \equiv 1$ (resp. $2 \pmod{p}$).¹ \square

The following lemma, valid for any $p > 2$ unramified, prime to η , will be especially useful to us (from [Wa, § 5.5, proof of Theorem 5.31]):

Lemma 2.2. *Let $\eta \in K^\times$, prime to p , and let $\lambda(\sigma)$, $\sigma \in G$, be p -integer coefficients of $K\mathbb{Q}_p$, not all divisible by p . Suppose that we have the relation of dependence modulo p^{N+1} , $N \geq 1$, of the n vectors $\ell_\sigma := (\dots, \log_p(\eta^{\tau\sigma^{-1}}), \dots)_\tau$, $\sigma \in G$,*

$$\sum_{\sigma \in G} \lambda(\sigma) \log_p(\eta^{\tau\sigma^{-1}}) \equiv 0 \pmod{p^{N+1}} \text{ for all } \tau \in G.$$

Then there exist coefficients $\lambda'(\sigma) \in \mathbb{Z}_{(p)}$, not all divisible by p , fulfilling the relation

$$\sum_{\sigma \in G} \lambda'(\sigma) \log_p(\eta^{\tau\sigma^{-1}}) \equiv 0 \pmod{p^{N+1}} \text{ for all } \tau \in G.$$

Taking $\tau = 1$ yields the relation $\sum_{\sigma \in G} \lambda'(\sigma) \alpha_p(\eta)^{\sigma^{-1}} \equiv 0 \pmod{p}$.

Proof. Modulo p^{N+1} , we can suppose that $\lambda(\sigma) \in Z_{K,(p)}$ for all $\sigma \in G$. Here the $\log_p(\eta^{\tau\sigma^{-1}})$ are also represented, modulo p^{N+1} , by elements of $Z_{K,(p)}$ and the corresponding linear algebra is a priori over the field K .

We obtain (for instance) $\mathrm{Tr}_{K/\mathbb{Q}}(\lambda(1)) \equiv 1 \pmod{p}$ by multiplication of the congruence by a suitable $u \in K^\times$ prime to p (Lemma 2.1). By conjugation with $\nu \in G$ we obtain $\sum_{\sigma \in G} \lambda(\sigma)^\nu \log_p(\eta^{\nu\tau\sigma^{-1}}) \equiv 0 \pmod{p^{N+1}}$ for all $\tau \in G$, which is equivalent to $\sum_{\sigma \in G} \lambda(\sigma)^\nu \log_p(\eta^{s\sigma^{-1}}) \equiv 0 \pmod{p^{N+1}}$ for all $s \in G$. Taking the trace in K/\mathbb{Q} of the coefficients (summation over ν), we obtain the rational p -integers $\lambda'(\sigma)$ for all $\sigma \in G$, with $\lambda'(1) \equiv 1 \pmod{p}$. \square

We may suppose that such linear relations of dependence modulo $p^{N+1}Z_K\mathbb{Z}_p$, for $N \geq 1$, are with coefficients in $\mathbb{Z}_{(p)}$ because the two notions of rank coincide. Taking the limit on N , one goes from the complete ring $Z_K\mathbb{Z}_p$ to the p -adic ring \mathbb{Z}_p .

2.1.3. Regulators. Let F be the $\mathbb{Z}[G]$ -module generated by η . Since $\mathbb{Q}_p \mathrm{Log}_p(F)$ is the $\mathbb{Q}_p[G]$ -module generated by $\mathrm{Log}_p(\eta)$ and since $\prod_{v \mid p} K_v$ is the representation of G induced by the representation K_{v_0} of the decomposition group $D_{\mathfrak{p}_0}$, the p -adic rank $r_p(F)$ of F is equal to the \mathbb{Q}_p -rank of the system of vectors $(\dots, \log_p(\eta^{\tau\sigma^{-1}}), \dots)_\tau$, $\sigma \in G$, then to the rank (in the usual sense from the lemmas) of the classical p -adic regulator $\mathcal{R}_p(\eta)$ (or Frobenius determinant) of η

$$\mathcal{R}_p(\eta) := \mathrm{Frob}^G(\log_p(\eta)) := \det(\log_p(\eta^{\tau\sigma^{-1}}))_{\sigma, \tau \in G}.$$

¹ For $p = 2$, $K = \mathbb{Q}(\sqrt{17})$, $\lambda = 1 + 2\sqrt{17}$, there is no solution u prime to 2.

The $\mathbb{Z}[G]$ -module F is monogenic in the framework recalled in [J, § 1], or [Gr1, III.3.1.2 (ii)], in which case the conjecture of Jaulent ([J, § 2]), asserts that the p -adic rank $\text{rg}_p(F)$ of F is equal to its \mathbb{Z} -rank $\text{rg}(F) := \dim_{\mathbb{Q}}(F \otimes \mathbb{Q})$ (this is the natural extension of the Leopoldt conjecture on the group of units of K).

We note that any minor of order r is divisible by p^r since $\log_p(\eta) \equiv -p \alpha_p(\eta) \pmod{p^2}$ in \mathbb{Z}_p . Hence the following definitions for $\eta \in K^\times$ prime to p :

Definitions 2.3. (i) Consider (for $p > 2$, unramified in K) the determinant

$$\text{Reg}_p^G(\eta) := \text{Frob}^G\left(\frac{-1}{p} \log_p(\eta)\right) := \det\left(\frac{-1}{p} \log_p(\eta^{\tau\sigma^{-1}})\right)_{\sigma, \tau \in G},$$

with integer coefficients of $K\mathbb{Q}_p$. This Frobenius determinant is called, in all the paper, the *normalized p -adic regulator of η* . We have $\text{Reg}_p^G(\eta) \equiv \Delta_p^G(\eta) \pmod{p}$, where

$$\Delta_p^G(\eta) := \text{Frob}^G(\alpha_p(\eta)) = \det(\alpha_p(\eta)^{\tau\sigma^{-1}})_{\sigma, \tau \in G}$$

is called the local regulator of η (cf. § 2.3).

(ii) For a real Galois field K , the usual p -adic regulator $\mathcal{R}_p(K)$ of the units is given by a minor of order $n - 1$ of $\text{Frob}^G(\log_p(\varepsilon)) = \det(\log_p(\varepsilon^{\tau\sigma^{-1}}))_{\sigma, \tau \in G}$, where ε is a suitable Minkowski unit, and the p -adic integer

$$p^{-(n-1)} \cdot \mathcal{R}_p(K) = \det\left(\frac{-1}{p} \log_p(\varepsilon^{\tau\sigma^{-1}})\right)_{\sigma \neq 1, \tau \neq 1}$$

is called the normalized p -adic regulator of K .

From Lemma 2.2 and after division by p of the logarithms, we are reduced to linear algebra reasoning over $\mathbb{Z}/p^N\mathbb{Z}$, $N \geq 1$; in particular, $\text{rg}_p(F)$ is the $\mathbb{Z}/p^N\mathbb{Z}$ -rank of the matrix $(\frac{-1}{p} \log_p(\eta^{\tau\sigma^{-1}}) \pmod{p^N})_{\sigma, \tau \in G}$, for N large enough.

If a minor M of order $\text{rg}(F)$ is nonzero modulo p^N , then it gives $\text{rg}_p(F)$, and it is the chosen practical viewpoint that we shall limit to $N = 1$, hence to the $\alpha_p(\eta)$ modulo p ; in this case, $\text{rg}_p(F)$ is a priori greater or equal to the $\mathbb{Z}/p\mathbb{Z}$ -rank of the matrix $(\alpha_p(\eta)^{\tau\sigma^{-1}} \pmod{p})_{\sigma, \tau \in G}$. If $\text{rg}(F) = n$, then the Leopoldt–Jaulent conjecture gives $\det(\frac{-1}{p} \log_p(\eta^{\tau\sigma^{-1}}))_{\sigma, \tau \in G} \sim p^e$, $e \geq 0$.

2.1.4. Strong form of the Leopoldt–Jaulent conjecture. The previous local point of view (for all p except a finite number) can be analyzed in the following two manners:

(a) *Local analysis.* We make no assumption on $\text{rg}(F)$. If there exists in F a relation $\prod_{\sigma \in G} (\eta^{\sigma^{-1}})^{\lambda(\sigma)} = \zeta$ (root of unity), $\lambda(\sigma) \in \mathbb{Z}$ not all zero (i.e., $\text{rg}(F) < n$), then for all p , prime to η , we have $\sum_{\sigma \in G} \lambda(\sigma) \log_p(\eta^{\sigma^{-1}}) = 0$ (i.e., $\text{rg}_p(F) < n$). These global relations are transmitted into the weaker local relations $\sum_{\sigma \in G} \lambda(\sigma) \alpha_p(\eta)^{\sigma^{-1}} \equiv 0 \pmod{p}$; they are said to be trivial (they do not come from a numerical circumstance with coefficients depending on the considered prime p , but to the existence of a non trivial *global relation* in F given by some constants $\lambda(\sigma) \in \mathbb{Z}$).

Conversely, if we have for fixed integers $\lambda(\sigma) \in \mathbb{Z}$, not all zero, the family of local conditions (for all p except a finite number)

$$\left(\sum_{\sigma \in G} \lambda(\sigma) \alpha_p(\eta)^{\sigma^{-1}} \equiv 0 \pmod{p} \right)_p, \quad (*)$$

the question is to know if this is globalisable under the form $\prod_{\sigma \in G} (\eta^{\sigma^{-1}})^{\lambda(\sigma)} = \zeta$.

We assume only the congruences $\sum_{\sigma \in G} \lambda(\sigma) \alpha_p(\eta)^{\sigma^{-1}} \equiv 0 \pmod{p}$ for all p except a finite number, with some $\lambda(\sigma) \in \mathbb{Z}$, not all zero and independent of p .

Let $\eta_0 := \prod_{\sigma \in G} (\eta^{\sigma^{-1}})^{\lambda(\sigma)} \in F$; then $\log_p(\eta_0) \equiv 0 \pmod{p^2}$ (i.e., $\text{Log}_p(\eta_0) \equiv 0 \pmod{p^2}$) and η_0 is, in $\prod_{v|p} K_v^\times$, of the form $\xi(1 + \beta p)^p$, β p -integer of $\prod_{v|p} K_v$ and ξ of torsion (of prime to p order, for p large enough); so $\eta_0 \in \prod_{v|p} K_v^{\times p}$ for almost all p . Conjecturally, η_0 is a root of unity of K (from Conjecture 8.5).

(b) *Global analysis.* By comparison, suppose that, in a projective limit framework, we have coefficients $\hat{\lambda}(\sigma) \in \hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$, such that

$$\sum_{\sigma \in G} \hat{\lambda}_p(\sigma) \text{Log}_p(\eta^{\sigma^{-1}}) = 0, \text{ for all } p \text{ prime to } \eta,$$

where for all $\sigma \in G$, $\hat{\lambda}_p(\sigma)$ is the p -component of $\hat{\lambda}(\sigma)$.

Let $i := (i_v)_{v, v(\eta)=0}$ be the diagonal embedding $F \otimes \hat{\mathbb{Z}} \rightarrow \hat{U}$, where

$$\hat{U} = \prod_{p, (p, \eta)=1} \left(\prod_{v|p} U_v^1 \times \prod_{v \nmid p, v(\eta)=0} \mu_p(K_v) \right),$$

$\mu_p(K_v)$ being the group of p th roots of unity in K_v and, for $v|p$,

$$U_v^1 = \mu_p(K_v) \times U', \text{ where } U' \text{ is } \mathbb{Z}_p\text{-free.}$$

We put $\hat{\eta}_0 := \prod_{\sigma \in G} (\eta^{\sigma^{-1}})^{\hat{\lambda}(\sigma)} \in F \otimes \hat{\mathbb{Z}}$ and we denote by $\hat{\eta}_{0,p} = \prod_{\sigma \in G} (\eta^{\sigma^{-1}})^{\hat{\lambda}_p(\sigma)}$ the p -component of $\hat{\eta}_0$ (p prime to η). Since $\text{Log}_p(\hat{\eta}_{0,p}) = 0$ for all p prime to η , we have for all place v prime to η , $i_v(\hat{\eta}_0) = \xi_v$, where (generally) ξ_v is a root of unity of order a divisor of $\ell^{n_\ell} - 1$, where ℓ is the residue characteristic of v (the places $v|p$ of K such that ξ_v is of order divisible by p are finite in number). We can write

$$i(\hat{\eta}_0) \in i(F \otimes \hat{\mathbb{Z}}) \bigcap \prod_{p, (p, \eta)=1} \left(\prod_{v, v(\eta)=0} \mu_p(K_v) \right).$$

By using the analogue for F of the local-global characterization of the p -adic conjecture of Leopoldt–Jaulent ([J, § 2]; see also [Gr1, III.3.6.6] in the case of units), we can state (under this conjecture, same reasoning) that we have

$$i(F \otimes \hat{\mathbb{Z}}) \bigcap \prod_{p, (p, \eta)=1} \left(\prod_{v, v(\eta)=0} \mu_p(K_v) \right) = i(\mu(K)).$$

We deduce that $\hat{\eta}_{0,p}$ is a root of unity $\zeta_p \in K$ for all p prime to η .

If moreover we suppose that $\hat{\lambda}_p(\sigma) \equiv \lambda(\sigma) \pmod{p}$ for all $\sigma \in G$ and all p prime to η , where the $\lambda(\sigma)$ are given rational integers, then $\eta_0 \in F^\times$, defined by

$$\eta_0 := \prod_{\sigma \in G} (\eta^{\sigma^{-1}})^{\lambda(\sigma)},$$

is equal to $\hat{\eta}_{0,p}$ up to a local p th power at p , thus $\eta_0 \zeta_p^{-1} \in \prod_{v|p} K_v^{\times p}$; we obtain the situation of § (a) since, for all p large enough, $\zeta_p = 1$ and there is coincidence.

We can see our approach as a very important weakening to this classical p -adic context concerning the Leopoldt–Jaulent conjecture for all prime p ; but as consideration, to have non empty information of a p -adic nature, we have been obliged

to suppose the existence of the family of rational integers (not all zero) $(\lambda(\sigma))_{\sigma \in G}$ satisfying the relation (*).

2.1.5. General study project. Our purpose, in connection with the previous p -adic comments, is to see with what probability (a priori very small) the normalized regulators $\text{Reg}_p^G(\eta)$ of η (η fixed) are divisible by p ($p \rightarrow \infty$).

A normalized regulator $\text{Reg}_p^G(\eta)$ can be factorised by means of powers of χ -regulators $\text{Reg}_p^\chi(\eta)$ (for the irreducible rational characters χ of G). This factorization does not depend on p . On the other hand, one can factorize $\text{Reg}_p^\chi(\eta)$ by means of θ -components $\text{Reg}_p^\theta(\eta)$ (for the irreducible p -adic characters $\theta \mid \chi$); this factorization depends on the residue degree of p in the field of values of the absolutely irreducible characters $\varphi \mid \chi$ of G . Then we shall get the congruence

$$\text{Reg}_p^\theta(\eta) \equiv \Delta_p^\theta(\eta) \pmod{p}$$

where the local θ -regulator $\Delta_p^\theta(\eta)$ is the θ -component of $\Delta_p^G(\eta) = \text{Frob}^G(\alpha_p(\eta))$ (cf. § 2.3). We shall deduce a probabilistic study in order to apply the heuristic principle of Borell–Cantelli.

Remark 2.4. Lemma 3.8 shall allow us to reduce (modulo \mathbb{Q}^\times) to an $\eta \in Z_K$, what we suppose in numerical and Diophantine studies. When the integer η is fixed or varies in a small numerical neighborhood (*in an Archimedean meaning and not p -adic*) and when $p \rightarrow \infty$, we shall speak of *probability*, for instance $\text{Prob}(\text{Reg}_p^G(\eta) \equiv 0 \pmod{p})$; on the other hand, when p is fixed and η is the variable (defined modulo p^2 in our study), the probability coincides with the density of the numbers $\eta \in K^\times$ (prime to p) satisfying the property.

It is clear that densities are canonical and are computed by means of algebraic calculations. As *probabilities* are linked to *densities*, one can confuse the two notions as soon as they are at most $\frac{O(1)}{p^2}$, and then “excluded” from probabilistic considerations of the Borell–Cantelli principle.

On the other hand, in the case of densities $\frac{O(1)}{p}$, the distinction is necessary. The idea (developed in [Gr2] for ordinary Fermat quotients) is that, conjecturally, when η is given, these *probabilities* are less than *densities* when $p \rightarrow \infty$ and that, under the existence of a binomial law for $\text{Prob}(\Delta_p^\theta(z) \equiv 0 \pmod{p})$ (z running through a suitable set of residues modulo p), this probability is $\frac{O(1)}{p^{\log_2(p)/\log(c_0(\eta)) - O(1)}}$ instead of $\frac{O(1)}{p}$, where $c_0(\eta) = \max_{\nu \in G}(|\eta^\nu|)$, which suggests the finiteness of the number of cases (Theorem 1.1).

2.2. Representations and group determinants (Frobenius determinants).

We make no assumption on the Galois group G ; for this, we begin by a general recall in terms of representations (for a comprehensive course on representations and characters, see [Sel]; for the Abelian case, see [Wa] or [C]).

2.2.1. General notation. As $\mathbb{C}[G]$ is the regular representation, we have the isomorphism $\mathbb{C}[G] \simeq \bigoplus_\rho \deg(\rho) \cdot V_\rho$, where (ρ, V_ρ) runs through the set of absolutely irreducible representations of G and where $\deg(\rho)$ is the degree (\mathbb{C} -dimension of V_ρ). We denote by φ the character of ρ ; consequently, $\deg(\rho) = \varphi(1)$. We choose to index objects depending on ρ by the letter φ (e.g. V_φ) and to keep $\rho = \rho_\varphi$ as a homomorphism of G into $\text{End}(V_\varphi)$.

For the algebra $\mathbb{C}[G]$ of endomorphisms $E \in \mathbb{C}[G]$, acting on the basis $\{\nu, \nu \in G\}$ by multiplication $\nu \mapsto E \cdot \nu$, we have the isomorphism $\mathbb{C}[G] \simeq \bigoplus_{\varphi} \text{End}(V_{\varphi})$, with $\text{End}(V_{\varphi}) \simeq e_{\varphi} \mathbb{C}[G]$, where the $e_{\varphi} = \frac{\varphi(1)}{|G|} \sum_{\nu \in G} \varphi(\nu^{-1}) \nu$ are the central orthogonal idempotents of $\mathbb{C}[G]$.

For the decomposition of $e_{\varphi} \mathbb{C}[G]$ into a direct sum of $\varphi(1)$ irreducible representations, isomorphic to V_{φ} , we use the projectors coming from a matrix representation $M(\rho_{\varphi}(\nu)) = (a_{ij}^{\varphi}(\nu))_{i,j}$ ([Se1, § I.2.7])

$$\pi_i^{\varphi} = \frac{\varphi(1)}{n} \sum_{\nu \in G} a_{ii}^{\varphi}(\nu^{-1}) \nu, \quad i = 1, \dots, \varphi(1),$$

giving a system of (non central) orthogonal idempotents such that $e_{\varphi} = \sum_i \pi_i^{\varphi}$.

2.2.2. Recalls on group determinants (from [C]). Let G be a finite group and let $\text{Frob}^G(X) = \det(X_{\tau\sigma^{-1}})_{\sigma, \tau \in G}$ be the determinant of the group G , or Frobenius determinant, with indeterminates $X := (X_{\nu})_{\nu \in G}$. We then have the formula

$$\text{Frob}^G(X) = \prod_{\varphi} \det \left(\sum_{\nu \in G} X_{\nu} \rho_{\varphi}(\nu^{-1}) \right)^{\varphi(1)}.$$

Hence the existence of homogeneous polynomials $P^{\varphi}(X)$, of degrees $\varphi(1)$, such that

$$\text{Frob}^G(X) = \prod_{\varphi} P^{\varphi}(X)^{\varphi(1)}.$$

The specialization $X_{\nu} \mapsto \frac{-1}{p} \log_p(\eta^{\nu})$ leads to (Definitions 2.3)

$$\text{Reg}_p^G(\eta) := \text{Frob}^G \left(\frac{-1}{p} \log_p(\eta) \right) = \prod_{\varphi} \det \left(\sum_{\nu \in G} \frac{-1}{p} \log_p(\eta^{\nu}) \rho_{\varphi}(\nu^{-1}) \right)^{\varphi(1)},$$

and from $\text{Reg}_p^{\varphi}(\eta) := P^{\varphi} \left(\dots, \frac{-1}{p} \log_p(\eta^{\nu}), \dots \right) = \det \left(\sum_{\nu \in G} \frac{-1}{p} \log_p(\eta^{\nu}) \rho_{\varphi}(\nu^{-1}) \right)$,

we group into partial products associated with the characters χ and θ irreducible over \mathbb{Q} and \mathbb{Q}_p , respectively

$$\text{Reg}_p^{\chi}(\eta) = \prod_{\varphi | \chi} \text{Reg}_p^{\varphi}(\eta) \quad \& \quad \text{Reg}_p^{\theta}(\eta) = \prod_{\varphi | \theta} \text{Reg}_p^{\varphi}(\eta).$$

2.2.3. Practical calculation of the $P^{\varphi}(X)$. The polynomials $P^{\varphi}(X)$ are obtained in the following way: from the vectorial space $V = \mathbb{C}[G]$ (provided with the basis G), we consider the endomorphism of $V[X]$, $L(X) = \sum_{\nu \in G} X_{\nu} \nu^{-1}$, which is such that

$$\left(\sum_{\nu \in G} X_{\nu} \nu^{-1} \right) \cdot \tau = \sum_{\nu \in G} X_{\nu} \nu^{-1} \tau = \sum_{\sigma \in G} X_{\tau\sigma^{-1}} \sigma, \quad \forall \tau \in G.$$

So, the determinant of this endomorphism in the basis $\{\tau, \tau \in G\}$ is the Frobenius determinant (defined up to the sign).

Let $(\rho_{\varphi}, V_{\varphi})$ be the family of non isomorphic absolutely irreducible representations. We shall take for $\text{End}(V_{\varphi})$ the component $e_{\varphi} \mathbb{C}[G]$ associated with the character φ . We use the algebra isomorphism $\tilde{\rho} : V \rightarrow \prod_{\varphi} \text{End}(V_{\varphi})$ defined by

$$\sum_{\nu \in G} a(\nu) \nu^{-1} \mapsto \left(\sum_{\nu \in G} a(\nu) \rho_{\varphi}(\nu^{-1}) \right)_{\varphi}.$$

where $\rho_{\varphi}(\nu^{-1}) = e_{\varphi} \nu^{-1}$ in the previous identification. From the Maschke theorem, we get for the endomorphism $L(X)$

$$\det_V(L(X)) = \prod_{\varphi} (\det_{V_{\varphi}}(L^{\varphi}(X)))^{\varphi(1)},$$

where $L^{\varphi}(X) = \sum_{\nu \in G} X_{\nu} \rho_{\varphi}(\nu^{-1}) \in \text{End}(V_{\varphi}[X])$. We put

$$P^{\varphi}(X) := \det_{V_{\varphi}}(L^{\varphi}(X)).$$

With a matrix realization $M(\rho_{\varphi}(\nu)) = (a_{ij}^{\varphi}(\nu))_{i,j}$ of the $\rho_{\varphi}(\nu)$, the matrix associated with $L^{\varphi}(X)$ is $M^{\varphi}(X) = \left(\sum_{\nu \in G} a_{ij}^{\varphi}(\nu^{-1}) X_{\nu} \right)_{i,j}$, of determinant $P^{\varphi}(X)$.

Let g be the least common multiple of the orders of the elements of G ; it is known that representations are realizable over the field $C_g = \mathbb{Q}(\mu_g)$ of g th roots of unity ([Se1, § 12.3]). So, we may suppose that the $a_{ij}^{\varphi}(\nu)$ are p -integer algebraic numbers, for all p large enough (i.e., $P^{\varphi}(X) \in Z_{C_g, (p)}[X]$ for all φ).

Let $\Gamma := \text{Gal}(C_g/\mathbb{Q})$ (commutative). Given an absolutely irreducible representation $\rho_{\varphi} : G \mapsto \text{End}_{C_g}(V_{\varphi})$, we define its conjugates in the following Galois manner so that for all $s \in \Gamma$, ρ_{φ}^s is the representation $G \mapsto \text{End}_{C_g}(V_{\varphi^s}) \simeq e_{\varphi^s} C_g[G]$ of character φ^s defined by $\varphi^s(\nu) = (\varphi(\nu))^s$, for all $s \in \Gamma$. We have, for all $s \in \Gamma$, $\varphi^s(\nu) = \varphi(\nu^{\omega(s)})$, where ω is the character $\Gamma \rightarrow (\mathbb{Z}/g\mathbb{Z})^{\times}$ of the action of Γ on μ_g . We also put $\varphi^t(\nu) := \varphi(\nu^t)$ for all integer t prime to g (Γ -conjugation).

2.2.4. Rational and p -adic characters – Idempotents. We recall their practical determination.

(i) *Rational characters.* We put, for φ fixed

$$\chi = \sum_{s \in \text{Gal}(C/\mathbb{Q})} \varphi^s =: \sum_{\varphi | \chi} \varphi \quad \text{and} \quad P^{\chi}(X) := \prod_{s \in \text{Gal}(C/\mathbb{Q})} P^{\varphi^s}(X) =: \prod_{\varphi | \chi} P^{\varphi}(X),$$

where $C \subseteq C_g$ is the field of values of any \mathbb{Q} -conjugate of φ .

(ii) *p -adic characters.* If $p \nmid g$, denote, for χ fixed, by L and D the field and the decomposition group of p in C/\mathbb{Q} . Let $f = |D|$ be the residue degree of p in C/\mathbb{Q} and $h = [L : \mathbb{Q}]$ the number of prime ideals \mathfrak{p} above p in C (or L); thus $[C : \mathbb{Q}] = hf$.

Let $\varphi | \chi$. We put

$$\theta(\nu) := \sum_{s \in D} \varphi^s(\nu) \in L, \quad \text{for all } \nu \in G \quad \& \quad P^{\theta}(X) := \prod_{s \in D} P^{\varphi^s}(X) =: \prod_{\varphi | \theta} P^{\varphi}(X).$$

We fix one of the h prime ideals $\mathfrak{p} | p$ of L (we shall say that θ and \mathfrak{p} are associated). As $L_{\mathfrak{p}^t} = \mathbb{Q}_p$ for all $t \in \text{Gal}(C/\mathbb{Q})/D$, we have congruences of the form $\theta(\nu) \equiv r_{\mathfrak{p}^t}(\nu) \pmod{\mathfrak{p}^t}$ in L , $r_{\mathfrak{p}^t}(\nu) \in \mathbb{Z}$; the rationals $r_{\mathfrak{p}^t}(\nu)$ depend numerically of the residue images at \mathfrak{p}^t of the trace in C/L of the $\varphi(\nu)$.

If $\theta = \sum_{s \in D} \varphi^s$ and \mathfrak{p} are associated, the h conjugates of θ are the $\theta^t = \sum_{s \in D} (\varphi^t)^s$ and we have $\theta^t(\nu) \equiv r_{\mathfrak{p}^{t-1}}(\nu) \pmod{\mathfrak{p}}$ (or $\theta^{t-1}(\nu) \equiv r_{\mathfrak{p}^t}(\nu) \pmod{\mathfrak{p}}$). As the θ^t are seen in $\mathbb{Z}_p \subset L_{\mathfrak{p}}$, we shall write by abuse $\theta^t(\nu) \equiv r_{\mathfrak{p}^{t-1}}(\nu) \pmod{p}$.

For p fixed, the integer f depends only on χ and is called the residue degree of the characters φ, θ and χ . We have, by Γ -conjugation, $\varphi^{p^i}(\nu) = \varphi(\nu^{p^i}) = \varphi(\nu)^{s_p^i}$, where s_p is the Frobenius automorphism (of order f) in C/\mathbb{Q} .

(iii) *Idempotents.* We put $e_{\chi} = \sum_{\varphi | \chi} e_{\varphi}$ and $e_{\theta} = \sum_{\varphi | \theta} e_{\varphi}$; thus $e_{\chi} = \sum_{\theta | \chi} e_{\theta}$. The e_{θ} (resp. e_{χ}) give a fundamental system of orthogonal idempotents of $\mathbb{Q}_p[G]$ (resp. $\mathbb{Q}[G]$). We can replace \mathbb{Q}_p (resp. \mathbb{Q}) by \mathbb{Z}_p (resp. $\mathbb{Z}_{(p)}$) because $p \nmid g$.

From $P^\varphi(X) = \det_{V_\varphi}(L^\varphi(X))$ we deduce that $P^{\varphi^s}(X) = \det_{V_{\varphi^s}}(L^{\varphi^s}(X))$ where $L^{\varphi^s}(X) = \sum_{\nu \in G} X_\nu \rho_\varphi^s(\nu^{-1})$ is given via the $(a_{ij}^\varphi(\nu^{-1}))^s$, which defines the conjugate by s of the polynomial $P^\varphi(X)$ (i.e., of its coefficients).

Theorem 2.5. (i) For all p large enough, the polynomials $P^\chi(X)$ (resp. $P^\theta(X)$) have rational p -integer coefficients (resp. p -adic integer coefficients).

(ii) For all irreducible character φ , we have $P^\varphi(\dots, X_{\pi\nu}, \dots) = \zeta_\pi P^\varphi(\dots, X_\nu, \dots)$ for all $\pi \in G$, where $\zeta_\pi^g = 1$.

Proof. (i) As $P^\varphi(X) \in Z_{C,(p)}[X]$ for all $\varphi \mid \chi$, $P^\chi(X) = \prod_{s \in \text{Gal}(C/\mathbb{Q})} P^{\varphi^s}(X)$ is invariant by Galois. Likewise $P^\theta(X) = \prod_{s \in D} P^{\varphi^s}(X) \in L[X] \subset L_p[X] = \mathbb{Q}_p[X]$.

(ii) For $\pi \in G$ call $[\pi]$ the operator defined by $[\pi]X_\nu = X_{(\pi\nu)}$ for all $\nu \in G$. Then $[\pi]$ and $\tilde{\rho}: V[X] \rightarrow \prod_\varphi \text{End}(V_\varphi[X])$ commute; moreover, since ρ_φ is a homomorphism, we have the following formula

$$[\pi] \left(\sum_{\nu \in G} X_\nu \rho_\varphi(\nu^{-1}) \right) = \sum_{\nu \in G} X_{\pi\nu} \rho_\varphi(\nu^{-1}) = \left(\sum_{\nu \in G} X_\nu \rho_\varphi(\nu^{-1}) \right) \rho_\varphi(\pi).$$

Then, since the determinant of $\rho_\varphi(\pi) \in \text{End}(V_\varphi)$ is that of a diagonal matrix whose diagonal is formed of roots of unity, we get

$$\det \left([\pi] \left(\sum_{\nu \in G} X_\nu \rho_\varphi(\nu^{-1}) \right) \right) = \zeta_\pi \det \left(\sum_{\nu \in G} X_\nu \rho_\varphi(\nu^{-1}) \right),$$

where ζ_π is of order a divisor of the order of $\rho_\varphi(\pi)$ which is a divisor of g . \square

Corollary 2.6. For all $\pi \in G$ and all absolutely irreducible character φ , we have $P^\varphi(\dots, \alpha^{\pi\nu}, \dots) = \zeta_\pi P^\varphi(\dots, \alpha^\nu, \dots)$ by the specialization $X_\nu \mapsto \alpha^\nu$, $\alpha \in Z_K$.

Consequently, $P^\chi(\dots, \alpha^{\pi\nu}, \dots) = \pm P^\chi(\dots, \alpha^\nu, \dots)$ for all $\pi \in G$.²

In the same way, $P^\theta(\dots, \alpha^{\pi\nu}, \dots) = \zeta'_\pi P^\theta(\dots, \alpha^\nu, \dots)$ for all $\pi \in G$, where ζ'_π is of order a divisor of $g.c.d.(g, p-1)$.

2.2.5. Numerical determinants. In this section, there is no reference to a prime number p and the characters that we consider are absolutely irreducible or rational. The above leads to define the numerical χ -determinants of Frobenius of any $\alpha \in Z_K$ (i.e., independent of the given $\eta \in K^\times$).

Definition 2.7. Let G be a finite group and let $\text{Frob}^G(X)$ be the associated group determinant. The χ -determinants (with indeterminates and numerical) are by definition the expressions

$$\text{Frob}^\chi(X) = \prod_{\varphi \mid \chi} P^\varphi(X) \quad \text{and} \quad \text{Frob}^\chi(\alpha) = \prod_{\varphi \mid \chi} P^\varphi(\dots, \alpha^\nu, \dots),$$

so that $\text{Frob}^G(\alpha) = \prod_\chi (\text{Frob}^\chi(\alpha))^{\varphi(1)}$ (where $\varphi \mid \chi$ for each χ).

Example 2.8. In the case of the group $D_6 = \{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$, we have the following numerical χ -determinants

$$\text{Frob}^1(\alpha) = \alpha + \alpha^\sigma + \alpha^{\sigma^2} + \alpha^\tau + \alpha^{\tau\sigma} + \alpha^{\tau\sigma^2},$$

$$\text{Frob}^{\chi_1}(\alpha) = \alpha + \alpha^\sigma + \alpha^{\sigma^2} - \alpha^\tau - \alpha^{\tau\sigma} - \alpha^{\tau\sigma^2},$$

$$\begin{aligned} \text{Frob}^{\chi_2}(\alpha) = & \alpha^2 + \alpha^{2\sigma} + \alpha^{2\sigma^2} - \alpha^{2\tau} - \alpha^{2\tau\sigma} - \alpha^{2\tau\sigma^2} - \alpha\alpha^\sigma - \alpha^\sigma\alpha^{\sigma^2} - \alpha^{\sigma^2}\alpha \\ & + \alpha^\tau\alpha^{\tau\sigma} + \alpha^{\tau\sigma}\alpha^{\tau\sigma^2} + \alpha^{\tau\sigma^2}\alpha^\tau. \end{aligned}$$

² Sign + except if $\chi = \varphi$ is quadratic and $\varphi(\pi) = -1$.

The two last one are of the form $\text{Frob}' \cdot \sqrt{m}$, $\text{Frob}' \in \mathbb{Q}$, where $k = \mathbb{Q}(\sqrt{m})$ is the quadratic subfield of K and we neglect the factor \sqrt{m} ; but $\text{Frob}^{\chi_2}(\alpha)$ appears to the square in the determinant $\text{Frob}^G(\alpha)$ and the result is rational, which is not the case of $\text{Frob}^{\chi_1}(\alpha)$. This is specific of quadratic characters.

For computations, we can return to the matrix realizations ($C = \mathbb{Q}$, $\varphi = \chi_2$)

$$\begin{aligned} \rho_\varphi(1) &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, & \rho_\varphi(\sigma) &= \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, & \rho_\varphi(\sigma^2) &= \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \\ \rho_\varphi(\tau) &= \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}, & \rho_\varphi(\tau\sigma) &= \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, & \rho_\varphi(\tau\sigma^2) &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \end{aligned}$$

which leads (by specialization and by taking the determinant) to

$$\begin{aligned} \sum_{\nu \in G} X_\nu \rho_\varphi(\nu^{-1}) &= \begin{pmatrix} X_1 - X_{\sigma^2} + X_\tau - X_{\tau\sigma} & X_\sigma - X_{\sigma^2} - X_{\tau\sigma} + X_{\tau\sigma^2} \\ -X_\sigma + X_{\sigma^2} - X_\tau + X_{\tau\sigma^2} & X_1 - X_\sigma - X_\tau + X_{\tau\sigma} \end{pmatrix}, \\ \text{Frob}^{\chi_2}(\alpha) &= \begin{vmatrix} \alpha - \alpha^{\sigma^2} + \alpha^\tau - \alpha^{\tau\sigma} & \alpha^\sigma - \alpha^{\sigma^2} - \alpha^{\tau\sigma} + \alpha^{\tau\sigma^2} \\ -\alpha^\sigma + \alpha^{\sigma^2} - \alpha^\tau + \alpha^{\tau\sigma^2} & \alpha - \alpha^\sigma - \alpha^\tau + \alpha^{\tau\sigma} \end{vmatrix}. \end{aligned}$$

Still for χ_2 (of degree 2) and the representation $e_{\chi_2} \mathbb{Q}[G] \simeq 2V_\varphi$, there exist two orthogonal projectors π_1, π_2 , of sum $e_{\chi_2} = \frac{1}{3}(2 - \sigma - \sigma^2)$ (§ 2.2.1), which yields here

$$\pi_1 = \frac{1}{3}(1 - \sigma^2 + \tau - \tau\sigma) \quad \& \quad \pi_2 = \frac{1}{3}(1 - \sigma - \tau + \tau\sigma).$$

2.3. The local θ -regulators. Let $\eta \in K^\times$ be given and let p be large enough so that p is unramified in K , prime to $n = [K : \mathbb{Q}]$ and η .

2.3.1. Generalities. We fix an algebraic integer $\alpha \in Z_K$ defined by $\alpha \equiv \alpha_p(\eta) \pmod{p}$. We obtain the determinant, with coefficients in Z_K , defined modulo p

$$\Delta_p^G(\eta) := \text{Frob}^G(\alpha) = \det(\alpha^{\tau\sigma^{-1}})_{\sigma, \tau \in G} = \prod_{\chi} \prod_{\theta | \chi} \prod_{\varphi | \theta} P^\varphi(\dots, \alpha^\nu, \dots)^{\varphi(1)}.$$

If $\Delta_p^G(\eta) \notin \mathbb{Q}$, we find again the existence of a factor \sqrt{m} which comes from the resolvent of a quadratic character of G and that we neglect in the definitions of regulators.

Definition 2.9. For all p large enough and for each \mathbb{Q}_p -irreducible character θ of G , we call local θ -regulator of η , the p -adic integer defined by

$$\Delta_p^\theta(\eta) := \prod_{\varphi | \theta} P^\varphi(\dots, \alpha^\nu, \dots), \text{ for } \alpha \equiv \alpha_p(\eta) := \frac{1}{p}(\eta^{p^{n_p}-1} - 1) \pmod{p}.$$

For $\theta | \chi$ (χ fixed), the corresponding local θ -regulators depend on the splitting of p in C/\mathbb{Q} and there are $h = \frac{[C:\mathbb{Q}]}{f}$ such regulators, where f is their residue degree (§ 2.2.4 (ii)). These regulators are only defined modulo p .

Remark 2.10. In the same manner, we may write (for p large enough) that the normalized regulator $\text{Reg}_p^G(\eta)$ is equal to

$$\prod_{\chi} \text{Reg}_p^\chi(\eta)^{\varphi(1)} = \prod_{\theta} \text{Reg}_p^\theta(\eta)^{\varphi(1)},$$

where

$$\text{Reg}_p^\theta(\eta) = \prod_{\varphi | \theta} P^\varphi(\dots, \frac{1}{p} \log_p(\eta^\nu), \dots).$$

We then have the congruences

$$\text{Reg}_p^\theta(\eta) \equiv \Delta_p^\theta(\eta) \pmod{p};$$

so p divides $\text{Reg}_p^\theta(\eta)$ if and only if $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$; in this case, there exists $e \geq 1$ such that $p^{e\varphi(1)}$ divides $\text{Reg}_p^\theta(\eta)$ where at each time $\varphi \mid \theta$ (§ 2.2.2).

We shall speak of an extra p -divisibility if $e \geq 2$.

2.3.2. *Particular remarks.* (i) We have

$$\Delta_p^\chi(\eta) := N_{C/\mathbb{Q}}(P^\varphi(\dots, \alpha^\nu, \dots)) \in \mathbb{Z} \quad (\varphi \mid \chi \text{ fixed}),$$

with the convention on the notation $N_{C/\mathbb{Q}}$, especially when K and C are not linearly disjoint. We recall the quadratic exception for χ .

In the same way

$$\Delta_p^\theta(\eta) := N_{\mathfrak{p}}(P^\varphi(\dots, \alpha^\nu, \dots)),$$

where for $\mathfrak{p} \mid p$ in C , \mathfrak{p} associated with θ , $N_{\mathfrak{p}}$ denotes the absolute local norm (issued from $N_{C/L}$) in the completion of C at \mathfrak{p} ; we find again $\Delta_p^\chi(\eta)$ as a product of the correspondent local norms at p .

Same normic relations by replacing Δ_p by Reg_p and α by $\frac{-1}{p}\log_p(\eta)$.

(ii) If $H = \{\nu \in G, \varphi(\nu) = \varphi(1)\}$ is the kernel of $\varphi \mid \theta \mid \chi$ (which only depends on χ) and if K' is the subfield of K fixed by H , we have

$$\Delta_p^\theta(\eta) = \Delta_p^{\theta'}(N_{K/K'}(\eta))$$

where θ' is the faithful character resulting from θ . By replacing η by $\eta' := N_{K/K'}(\eta)$ one always can suppose that θ is a faithful character.

2.3.3. *Characters χ of degree 1, of order 1 or 2.* Let $\eta \in K^\times$ and let $\alpha \equiv \alpha_p(\eta) \pmod{p}$, $\alpha \in Z_K$.

(i) If $\chi = \theta = 1$, the θ -regulator corresponds to $N_{K/\mathbb{Q}}(\eta) = a \in \mathbb{Q}^\times$ and is given by $\text{Tr}_{K/\mathbb{Q}}(\alpha)$, in other words

$$\Delta_p^1(\eta) \equiv \frac{-1}{p}\log_p(a) \equiv \frac{1}{p}(a^{p-1} - 1) \equiv q_p(a) \pmod{p}$$

(Fermat quotient of a); for classical properties and use of Fermat quotients, see, e.g., [EM], [GM], [Gr2], [Hat], [H-B], [KR], [OS], [Si].

For $a = 659$ and $p \leq 10^9$, we only find the solutions $p = 23, 131, 2221, 9161, 65983$. See [Gr4, Pr. A-1]. For $a = 47$ and $a = 72$, we find no solution for $p \leq 10^{11}$.

(ii) If $\chi = \theta$ is quadratic and if $k = \mathbb{Q}(\sqrt{m})$ is the quadratic subfield of K fixed by the kernel of χ , we obtain a θ -regulator corresponding to the case $N_{K/k}(\eta) \in k^\times \setminus \mathbb{Q}^\times$; if $\text{Tr}_{K/k}(\alpha) =: u + v\sqrt{m} \in k$, it is given by

$$\Delta_p^\theta(\eta) \equiv (1 - \tau)(u + v\sqrt{m}) \equiv 2v\sqrt{m} \pmod{p}.$$

If K is a real quadratic field with the fundamental unit ε , because of the multiplicative relation of dependence $\varepsilon^{1+\sigma} = \pm 1$, the 1-regulators $\Delta_p^1(\varepsilon)$ are trivially zero modulo p . The θ -regulator of the quadratic character is $\Delta_p^\theta(\varepsilon) \equiv 2v\sqrt{m} \pmod{p}$ (computed via $\varepsilon^{p^{n_p}-1} \equiv 1 + pv\sqrt{m} \pmod{p^2}$).

We compute the θ -regulator $\Delta_p^\theta(\varepsilon)$ of the fundamental unit $\varepsilon = 5 + 2\sqrt{6}$, for all $p \leq 10^9$ ($p \neq 2, 3$) (see [Gr4, Pr. A-2] valuable for any quadratic integer). We find a θ -regulator equal to zero modulo p only for $p = 7, 523$, which gives a second observation on the rarity of the phenomenon.

Let $\eta = 1 + \sqrt{6}$ of norm -5 . We have $\text{rg}(F) = 2$ (no trivial nullities). We verify that Fermat quotients $\Delta_p^1(\eta)$ of -5 are all nonzero modulo p in the tested interval. The

solutions for $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$, $\theta \neq 1$, are $p = 11, 37, 163, 4219$. For $\eta = 1 + 5\sqrt{-1}$ of norm 26, we find for $\theta \neq 1$ the two solutions $p = 73, 12021953$. For the golden number $\frac{1+\sqrt{5}}{2}$ we find no solution in the tested interval.

2.3.4. Criterion of trivial nullity for local χ -regulators. Let $\eta \in K^\times$ and let F be the $\mathbb{Z}[G]$ -module generated by η .

Remark 2.11. In the decomposition $\text{Frob}^G(\alpha) = \prod_{\chi} \text{Frob}^\chi(\alpha)^{\varphi(1)}$, when $\alpha \equiv \alpha_p(\eta) \pmod{p}$, some of the local χ -regulators $\Delta_p^\chi(\eta)$ are zero modulo p as soon as there exists a non trivial global multiplicative relation of the form

$$\prod_{\nu \in G} (\eta^{\nu^{-1}})^{\lambda(\nu)} = 1, \quad \lambda(\nu) \in \mathbb{Z},$$

which yields $\sum_{\nu \in G} \lambda(\nu) \alpha^{\nu^{-1}} \equiv 0 \pmod{p}$ for all p prime to η .

Lemma 2.12. *If we have $\dim_{\mathbb{Q}}((F \otimes \mathbb{Q})^{e_\chi}) < \dim_{\mathbb{Q}}(e_\chi \mathbb{Q}[G]) = [C : \mathbb{Q}] \varphi(1)^2$ (i.e., there exists $U \in \mathbb{Q}[G]$ such that $\eta^{U_\chi} = 1$, with $U_\chi := e_\chi U \neq 0$), then the local χ -regulators $\Delta_p^\chi(\eta) := \text{Frob}^\chi(\alpha)$ are zero modulo p for all p large enough (they are said trivially null modulo p).*

This implies the trivial nullity modulo p of certain $\Delta_p^\theta(\eta)$, $\theta \mid \chi$, namely those for which $U_\theta := e_\theta U \not\equiv 0 \pmod{p}$; for the proof, see the Lemmas of § 3.2 (criterion of nullity modulo p of $\Delta_p^\theta(\eta)$).

Remarks 2.13. (i) If $\varphi(1) = 1$, $\Delta_p^\chi(\eta)$ trivially null modulo p is equivalent to $\eta^{e_\chi} = 1$ (i.e., $U_\chi = e_\chi$), in which case $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$ trivially for all $\theta \mid \chi$.

(ii) If $\varphi(1) > 1$, $\Delta_p^\chi(\eta)$ is trivially null modulo p if there exists i , $1 \leq i \leq \varphi(1)$, such that, in $F \otimes C$, we have $\eta^{\pi_i^\varphi} = 1$ for $\varphi \mid \chi$ (§ 2.2.1).

For instance, for $G = D_6$ and $\varphi = \chi = \chi_2$, the elements

$$\pi_1^\varphi = \frac{1}{3}(1 - \sigma^2 + \tau - \tau\sigma) \text{ and } \pi_2^\varphi = \frac{1}{3}(1 - \sigma - \tau + \tau\sigma)$$

are such that $e_\chi \pi_i^\varphi = \pi_i^\varphi$, $i = 1, 2$, $\pi_1^\varphi + \pi_2^\varphi = e_\chi$, and $\pi_1^\varphi \pi_2^\varphi = 0$ (cf. Example 2.8).

So we may have the non trivial φ -relation $\eta^{U_1} := \eta^{1-\sigma^2+\tau-\tau\sigma} = 1$ while $\eta^{U_2} := \eta^{1-\sigma-\tau+\tau\sigma} \neq 1$ (i.e., $\dim_{\mathbb{Q}}(F \otimes \mathbb{Q})^{e_\chi} = 2$ for $\dim_{\mathbb{Q}}(e_\chi \mathbb{Q}[G]) = 4$); we would have $\eta^{e_\chi \cdot (U_1+U_2)} = \eta^{3e_\chi} = \eta^{3U_2} \neq 1$, but we verify that the χ -regulator $\Delta_p^\chi(\eta)$ is equal to zero modulo p because of the first relation.

To suppose $\text{rg}(F) = n$ avoids this disadvantage. We can always suppose it by multiplying η by a suitable η' in such a way that $(FF') \otimes \mathbb{Q} \simeq \mathbb{Q}[G]$ and $F \cap F' = 1$ (obvious notation).

(iii) For $U \in \mathbb{Z}_{(p)}[G]$, we have $U_\chi = \sum_{\varphi \mid \chi} U_\varphi$ and $U_\varphi = e_\varphi U_\chi$. We have $U_\chi \equiv 0 \pmod{p}$ if and only if $U_\varphi \equiv 0 \pmod{p}$ for at least a (donc all) $\varphi \mid \chi$ (because the $\varphi \mid \chi$ are conjugate by $\text{Gal}(C/\mathbb{Q})$).

These congruences \pmod{p} in the group algebras mean (depending on the case)

$$(\text{mod } p \mathbb{Z}_{(p)}[G]) \quad \text{or} \quad (\text{mod } p Z_{C,(p)}[G])$$

where $Z_{C,(p)}$ is the ring of p -integers of the field of values C of the $\varphi \mid \chi$.

This does not occur for $U_\chi = \sum_{\theta|\chi} U_\theta$ and $U_\theta = e_\theta U_\chi$ because $U_\theta \equiv 0 \pmod{p}$ in $\mathbb{Z}_p[G]$ means $U_\theta \equiv 0 \pmod{\mathfrak{p}}$ in $L[G]$ (for θ and \mathfrak{p} associated), which is only equivalent to $U_\varphi \equiv 0 \pmod{\mathfrak{p}}$ for all $\varphi|\theta$ (§ 2.2.4 (ii)).

Examples 2.14. a) $G = C_n$. Let G cyclic of order n and let χ of order $d|n$; then the elements $\eta \in K^\times$ such that $\eta^{e_\chi} = 1$ correspond to the trivial nullity \pmod{p} of

$$\Delta_p^\chi(\eta) = N_{C/\mathbb{Q}}\left(\sum_{\nu \in G} \varphi(\nu^{-1}) \alpha^\nu\right).$$

For $n = 3$ (for which $C = \mathbb{Q}(j)$, where $j^3 = 1$, $j \neq 1$), we have the two rational idempotents

$$e_1 = \frac{1}{3}(1 + \sigma + \sigma^2), \quad e_\chi = \frac{1}{3}(2 - \sigma - \sigma^2).$$

(i) The $\eta \in K^\times$ such that $\eta^{e_1} = 1$ (i.e., of norm 1 in $F \otimes \mathbb{Q}$), correspond to the trivial nullity of $\Delta_p^1(\eta) = \alpha + \alpha^\sigma + \alpha^{\sigma^2}$.

(ii) The $\eta \in K^\times$ such that $\eta^{e_\chi} = 1$ or $N_{K/\mathbb{Q}}(\eta) = \eta^3$, hence such that $\eta \in \mathbb{Q}^\times$, correspond to the trivial nullity of $\Delta_p^\chi(\eta) = N_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha + j^2 \alpha^\sigma + j \alpha^{\sigma^2})$.

b) $G = D_6$. The three idempotents for the group D_6 are

$$\begin{aligned} e_1 &= \frac{1}{6}(1 + \sigma + \sigma^2 + \tau + \tau\sigma + \tau\sigma^2), \\ e_{\chi_1} &= \frac{1}{6}(1 + \sigma + \sigma^2 - (\tau + \tau\sigma + \tau\sigma^2)), \\ e_{\chi_2} &= \frac{1}{6}(2 - \sigma - \sigma^2). \end{aligned}$$

(i) The η such that $\eta^{e_1} = 1$ correspond to the trivial nullity of $\Delta_p^1(\eta) = \text{Tr}_{K/\mathbb{Q}}(\alpha)$.

(ii) The η such that $\eta^{e_{\chi_1}} = 1$ are such that $N_{K/k}(\eta) \in \mathbb{Q}^\times$, where k is the quadratic subfield of K , and correspond to the trivial nullity of

$$\Delta_p^{\chi_1}(\eta) = \alpha + \alpha^\sigma + \alpha^{\sigma^2} - \alpha^\tau - \alpha^{\tau\sigma} - \alpha^{\tau\sigma^2} = (1 - \tau) \text{Tr}_{K/k}(\alpha).$$

(iii) The η such that $\eta^{U_{\chi_2}} = 1$ for $U_{\chi_2} \in e_{\chi_2} \mathbb{Q}[G] \setminus \{0\}$ lead to the trivial nullity of

$$\begin{aligned} \Delta_p^{\chi_2}(\eta) &= \alpha^2 + \alpha^{2\sigma} + \alpha^{2\sigma^2} - \alpha^{2\tau} - \alpha^{2\tau\sigma} - \alpha^{2\tau\sigma^2} - \alpha\alpha^\sigma - \alpha^\sigma\alpha^{\sigma^2} - \alpha^{\sigma^2}\alpha \\ &\quad + \alpha^\tau\alpha^{\tau\sigma} + \alpha^{\tau\sigma}\alpha^{\tau\sigma^2} + \alpha^{\tau\sigma^2}\alpha^\tau. \end{aligned}$$

3. \mathbb{F}_p -LINEAR RELATIONS BETWEEN THE CONJUGATES OF α

Let $\eta \in K^\times$ be fixed and let p be a large enough prime number.

Let $\alpha_p(\eta) := \frac{1}{p}(\eta^{p^{n_p}-1} - 1) \in Z_{K,(p)}$. We intend to establish the relation between the nullity modulo p of certain $\Delta_p^\theta(\eta)$ and the existence of certain \mathbb{F}_p -linear relations between the conjugates of $\alpha_p(\eta)$ modulo p . We implicitly suppose $\text{rg}(F) = n$. First, let us establish elementary generalities:

3.1. \mathbb{F}_p -independence. Let $\alpha \in K$, arbitrary (so $\alpha \in Z_{K,(p)}$ for all p large enough). We shall say that the α^ν , $\nu \in G$, are \mathbb{F}_p -independent if, for all family of coefficients $u(\nu) \in \mathbb{Z}_{(p)}$, the congruence $\sum_{\nu \in G} u(\nu) \alpha^{\nu^{-1}} \equiv 0 \pmod{p}$, in $Z_{K,(p)}$, implies $u(\nu) \equiv 0 \pmod{p}$ for all $\nu \in G$.

We then have the following result where we recall that $\text{Frob}^G(\alpha) = \det(\alpha^{\tau\sigma^{-1}})_{\sigma, \tau \in G}$:

Proposition 3.1. *Let $\alpha \in K$ be given. We assume p large enough in such a way that $\alpha \in Z_{K,(p)}$ and p does not divide the discriminant of K .*

- (i) *The α^ν are \mathbb{F}_p -independent if and only if α is a normal $\mathbb{Z}_{(p)}$ -basis of $Z_{K,(p)}$.*
- (ii) *The α^ν are \mathbb{F}_p -independent if and only if $\text{Frob}^G(\alpha)$ is prime to p .*

Proof. (i) If α is a normal $\mathbb{Z}_{(p)}$ -basis of $Z_{K,(p)}$, any congruence $\sum_{\nu \in G} u(\nu) \alpha^{\nu^{-1}} \equiv 0 \pmod{p}$, $u(\nu) \in \mathbb{Z}_{(p)}$, leads to $u(\nu) \equiv 0 \pmod{p}$, for all $\nu \in G$.

Assume now that the α^ν are \mathbb{F}_p -independent and that there exists a non-trivial relation of \mathbb{Q} -linear dependence between the conjugates of α ;

it follows a relation of the form $\sum_{\nu \in G} r(\nu) \alpha^{\nu^{-1}} = 0$ with integers $r(\nu)$, not all zero,

such that $\text{p.g.c.d.}(r(\nu))_\nu = 1$; whence $r(\nu) \equiv 0 \pmod{p}$ for all $\nu \in G$ (absurd).

Consequently α is yet a normal \mathbb{Q} -basis of K . If $\beta \in Z_{K,(p)} \setminus \{0\}$, there exist some $r(\nu) \in \mathbb{Z}$, not all zero, and an integer d , prime to $\text{p.g.c.d.}(r(\nu))_\nu$, such that $d\beta = \sum_{\nu \in G} r(\nu) \alpha^{\nu^{-1}}$. We have $p \nmid d$ otherwise the $r(\nu)$ should be divisible by p .

Thus α is a normal $\mathbb{Z}_{(p)}$ -basis of $Z_{K,(p)}$.

(ii) Suppose that the α^ν are \mathbb{F}_p -independent; as $\alpha = \frac{1}{d}\beta$, $\beta \in Z_K \setminus pZ_K$, $d \in \mathbb{Z} \setminus p\mathbb{Z}$, one can return to the integer case for α . As p is large enough, it does not divide the discriminant of K/\mathbb{Q} , and the discriminant of the normal $\mathbb{Z}_{(p)}$ -basis α , of $Z_{K,(p)}$, is prime to p (indeed, the conductor $\mathfrak{f} \in \mathbb{Z}$ such that $\mathfrak{f}Z_K \subseteq \bigoplus_\nu \mathbb{Z} \alpha^\nu$ is not divisible by p and the two discriminants coincide up to a p -adic unit). But the discriminant of the normal basis α is the square of the Frobenius determinant $\text{Frob}^G(\alpha) = \det(\alpha^{\tau\sigma^{-1}})_{\sigma,\tau \in G}$.

Suppose $\text{Frob}^G(\alpha)$ prime to p , and suppose there exist some $\lambda(\sigma) \in \mathbb{Z}_{(p)}$, not all divisible by p , such that $\sum_{\sigma \in G} \lambda(\sigma) \alpha^{\sigma^{-1}} \equiv 0 \pmod{p}$. By conjugation by $\tau \in G$, we obtain a $\mathbb{Z}_{(p)}$ -linear relation over the lines of the form

$$\sum_{\sigma \in G} \lambda(\sigma) (\dots, \alpha^{\tau\sigma^{-1}}, \dots)_\tau \equiv (\dots, 0, \dots)_\tau \pmod{p},$$

whence $\text{Frob}^G(\alpha) \equiv 0 \pmod{p}$ (absurd). \square

Corollary 3.2. *If for p large enough at least one of the local θ -regulators $\Delta_p^\theta(\eta)$ is zero modulo p , then the $\alpha_p(\eta)^\nu$ are not \mathbb{F}_p -independent and there exists a \mathbb{F}_p -linear relation $\sum_{\nu \in G} u(\nu) \alpha_p(\eta)^{\nu^{-1}} \equiv 0 \pmod{p}$, with $u(\nu) \in \mathbb{Z}_{(p)}$ not all divisible by p .*

3.2. Criterion of nullity modulo p of the $\Delta_p^\theta(\eta)$. We refer to § 2.2.4 using the decomposition field L of p in C/\mathbb{Q} and $D = \text{Gal}(C/L)$. To simplify, we suppose $K \cap C = \mathbb{Q}$. We recall that $Z_{C,(p)}$ is the ring of p -integers of C .

3.2.1. Main lemmas. Let $\eta \in K^\times$ be such that the multiplicative $\mathbb{Z}[G]$ -module generated by η is of \mathbb{Z} -rank n . We fix $\alpha \equiv \alpha_p(\eta) \pmod{p}$ in Z_K . As usual, φ denotes an absolutely irreducible character and θ an irreducible p -adic character.

Definition 3.3. (i) If $\sum_{\nu \in G} u(\nu) \alpha^{\nu^{-1}} \equiv 0 \pmod{p}$, $u(\nu) \in \mathbb{Z}_{(p)}$ for all $\nu \in G$, we call *associated relation with α* the element

$$U = \sum_{\nu \in G} u(\nu) \nu^{-1} \in \mathbb{Z}_{(p)}[G],$$

and we define, for characters φ and θ , the φ -relations $U_\varphi := e_\varphi \cdot U \in Z_{C,(p)}[G]$, and the θ -relations $U_\theta := e_\theta \cdot U \in Z_{L,(p)}[G]$.

(ii) We denote by \mathcal{L} the G -module of the relations $U \in \mathbb{Z}_{(p)}[G]$ (defined modulo $p\mathbb{Z}_{(p)}[G]$), associated with α . Seen in $\mathbb{F}_p[G]$, we have $\mathcal{L} = \{0\}$ if and only if the α^ν are \mathbb{F}_p -independent (§ 3.1) and we have $\mathcal{L} = \mathbb{F}_p[G]$ if and only if $\alpha \equiv 0 \pmod{p}$.

(iii) For θ , we denote by $\mathcal{L}^\theta \simeq \delta V_\theta$ the θ -component $e_\theta \mathcal{L}$, where V_θ (of \mathbb{F}_p -dimension $f\varphi(1)$) is the irreducible representation of character θ ; then $0 \leq \delta \leq \varphi(1)$.

(iv) Let $\mathfrak{p} | p$ the prime ideal of L associated with θ . Thus $\theta(\nu) = \sum_{s \in D} \varphi^s(\nu) \in Z_{L,(p)}$ is defined via $\theta(\nu) \equiv r_{\mathfrak{p}}(\nu) \pmod{\mathfrak{p}}$, $r_{\mathfrak{p}}(\nu) \in \mathbb{Z}$; if $U \in \mathbb{Z}_{(p)}[G]$, $U_\theta \in Z_{L,(p)}[G]$ is congruent modulo \mathfrak{p} to an element of $\mathbb{Z}_{(p)}[G]$. We shall view U_θ in $\mathbb{Z}_p[G] \pmod{p}$ or in $Z_{L,(p)}[G] \pmod{\mathfrak{p}}$ depending on the context (see Remark 2.13).

Let $U = \sum_{\nu \in G} u(\nu) \nu^{-1} \in \mathbb{Z}_{(p)}[G]$; then $U_\varphi = \sum_{\nu \in G} u_\varphi(\nu) \nu^{-1} \in Z_{C,(p)}[G]$, with $u_\varphi(\nu) = \frac{\varphi(1)}{n} \sum_{\tau \in G} \varphi(\tau^{-1}) u(\nu\tau)$. We then have $U_\theta = \sum_{\varphi | \theta} U_\varphi$.

Lemma 3.4. *If $U = \sum_{\nu \in G} u(\nu) \nu^{-1} \in \mathcal{L}$, then $U_\varphi \cdot \alpha := \sum_{\nu \in G} u_\varphi(\nu) \alpha^{\nu^{-1}} \equiv 0 \pmod{p}$ for all irreducible character φ .*

Proof. We have $U_\varphi \cdot \alpha = \frac{\varphi(1)}{n} \sum_{\tau \in G} \varphi(\tau^{-1}) \left(\sum_{\sigma \in G} u(\sigma) \alpha^{\tau\sigma^{-1}} \right) \equiv 0 \pmod{p}$, by conjugation by τ of $\sum_{\sigma \in G} u(\sigma) \alpha^{\sigma^{-1}} \equiv 0 \pmod{p}$. \square

Lemma 3.5. *Let $U \in \mathcal{L}$, let \mathfrak{p} be associated with θ , and let $\varphi | \theta$ be such that $U_\varphi \not\equiv 0 \pmod{\mathfrak{p}}$ (condition independent of the choice of $\varphi | \theta$). Then the endomorphism $E_\varphi := e_\varphi \sum_{\nu \in G} \alpha^\nu \nu^{-1}$ of $\text{End}_{KC}(V_\varphi)$ is not invertible modulo \mathfrak{p} .*

Proof. Let us work by transposition of endomorphisms (which does not change determinants). We have

$$\begin{aligned} U_\varphi \cdot E_\varphi &= e_\varphi \sum_{\nu \in G} U_\varphi \alpha^\nu \nu^{-1} = e_\varphi \sum_{\nu \in G} \alpha^\nu \sum_{\sigma \in G} u_\varphi(\sigma) \sigma^{-1} \nu^{-1} \\ &= e_\varphi \sum_{\tau \in G} \left(\sum_{\nu \in G} u_\varphi(\nu^{-1} \tau) \alpha^\nu \right) \tau^{-1} = e_\varphi \sum_{\tau \in G} (U_\varphi \cdot \alpha)^\tau \tau^{-1} \equiv 0 \pmod{p}, \end{aligned}$$

from Lemma 3.4 above. \square

As E_φ is an endomorphism of V_φ over KC , for the prime ideal $\mathfrak{p} | p$ of C such that $U_\varphi \not\equiv 0 \pmod{\mathfrak{p}}$, there exists a prime ideal $\mathfrak{P} | \mathfrak{p}$ of KC for which $\det(E_\varphi) \equiv 0 \pmod{\mathfrak{P}}$. But any conjugation by $\tau \in G$ gives

$$E_\varphi^\tau = e_\varphi \sum_{\nu \in G} \alpha^{\tau\nu} \nu^{-1} = e_\varphi \sum_{\nu \in G} \alpha^\nu \nu^{-1} \cdot (e_\varphi \tau) = E_\varphi \circ e_\varphi \tau,$$

and we obtain $\det(E_\varphi^\tau) = \det(E_\varphi) \det(e_\varphi \tau) \equiv 0 \pmod{\mathfrak{P}^\tau}$, whence $\det(E_\varphi) \equiv 0 \pmod{\prod_{\tau \in G} \mathfrak{P}^\tau}$ since the $\det(e_\varphi \tau)$ are invertible.

Since $\det(E_\varphi) \equiv 0 \pmod{\mathfrak{p}}$ (extended to KC), this yields $P^\varphi(\dots, \alpha^\nu, \dots) \equiv 0 \pmod{\mathfrak{p}}$ which may be written $\Delta_p^\varphi(\eta) \equiv 0 \pmod{\mathfrak{p}}$. Since $\Delta_p^\theta(\eta)$ is the local norm at \mathfrak{p} of $\Delta_p^\varphi(\eta)$, we get:

Corollary 3.6. *If $U_\varphi \not\equiv 0 \pmod{\mathfrak{p}}$, we have $\Delta_p^\theta(\eta) \equiv 0 \pmod{\mathfrak{p}^f}$ (or modulo p^f in $L_{\mathfrak{p}} = \mathbb{Q}_p$) for the p -adic character θ above φ associated with \mathfrak{p} .*

Lemma 3.7. *Reciprocally, if $E_\varphi := e_\varphi \sum_{\nu \in G} \alpha^\nu \nu^{-1} \in \text{End}_{KC}(V_\varphi)$ is not invertible modulo \mathfrak{p} , there exists a nonzero φ -relation modulo \mathfrak{p} of the form $W = \sum_{\sigma \in G} w(\sigma) \sigma^{-1}$ in $e_\varphi Z_{C,(p)}[G]$, such that $W \cdot \alpha \equiv 0 \pmod{\mathfrak{p}}$.*

Proof. Lemma 2.2 allowing $Z_{C,(p)}$ -linear reasoning, there exists $W \in e_\varphi Z_{C,(p)}[G]$ such that $W \not\equiv 0 \pmod{\mathfrak{p}}$ is in the kernel of the transposed of E_φ , which may be written $W \cdot E_\varphi \cdot \equiv 0 \pmod{\mathfrak{P}}$ for $\mathfrak{P} | \mathfrak{p}$ in KC .

The relation $E_\varphi^\tau = E_\varphi \circ e_\varphi \tau$ and the fact that W is with coefficients in $Z_{C,(p)}$ shows, by conjugations, that the congruence occurs modulo \mathfrak{p} (extended).

Put $W = \sum_{\sigma \in G} w(\sigma) \sigma^{-1}$, $w(\sigma) \in Z_{C,(p)}$ for all $\sigma \in G$; the congruence $W \cdot E_\varphi \equiv 0 \pmod{\mathfrak{p}}$ may be written successively (since $e_\varphi W = W$)

$$\begin{aligned} \sum_{\nu \in G} \sum_{\sigma \in G} w(\sigma) \alpha^\nu \sigma^{-1} \nu^{-1} &\equiv \sum_{\sigma \in G} w(\sigma) \sum_{t \in G} \alpha^{t^{-1} \sigma^{-1}} t \equiv 0 \pmod{\mathfrak{p}}, \\ \sum_{t \in G} \left(\sum_{\sigma \in G} w(\sigma) \alpha^{t^{-1} \sigma^{-1}} \right) t &\equiv 0 \pmod{\mathfrak{p}}; \end{aligned}$$

so $\sum_{\sigma \in G} w(\sigma) \alpha^{t^{-1} \sigma^{-1}} \equiv 0 \pmod{\mathfrak{p}}$, for all $t \in G$, whence $\sum_{\sigma \in G} w(\sigma) \alpha^{\sigma^{-1}} \equiv 0 \pmod{\mathfrak{p}}$, giving the non-trivial associated φ -relation modulo \mathfrak{p}

$$W = \sum_{\sigma \in G} w(\sigma) \sigma^{-1} \in e_\varphi Z_{C,(p)}[G],$$

such that $W \cdot \alpha \equiv 0 \pmod{\mathfrak{p}}$ (but W is not necessarily in $e_\varphi \mathbb{Z}_{(p)}[G]$). \square

Lemma 3.8. *In the study of the $\Delta_p^\theta(\eta)$, $\theta \neq 1$, one may suppose $\eta \in Z_K$.*

Proof. Put $\eta = \mu \cdot d^{-1}$, $\mu \in Z_K$, $d \in \mathbb{Z}$. We have $\alpha_p(\eta) \equiv \alpha_p(\mu) - \alpha_p(d) \pmod{p}$, and $\sum_{\nu \in G} u(\nu) \alpha_p(\eta)^{\nu^{-1}} \equiv \sum_{\nu \in G} u(\nu) \alpha_p(\mu)^{\nu^{-1}} \pmod{p}$, for all θ -relations relative to η , because $\alpha_p(d)$ is invariant by Galois and $\theta \neq 1$; whence $\mathcal{L}^\theta(\eta) = \mathcal{L}^\theta(\mu)$ and $\Delta_p^\theta(\eta)$ & $\Delta_p^\theta(\mu)$ null (or not) at the same time (Theorem 3.9 below). \square

Then we shall suppose $\eta \in Z_K$ for certain Diophantine reasoning (essentially in Sections 6, 7), but we can keep $\eta \in K^\times$ in general statements.

3.2.2. *Main statement.* The technical results of § 3.2.1 lead to the following:

Theorem 3.9. *Let K/\mathbb{Q} be a Galois extension of degree n of Galois group G . Let $\eta \in K^\times$ be such that the multiplicative $\mathbb{Z}[G]$ -module generated by η is of \mathbb{Z} -rank n . For any unramified prime $p > 2$, prime to n and η , put $\eta_1 := \eta^{p^{n_p}-1} = 1 + p \alpha_p(\eta)$, $\alpha_p(\eta) \in Z_{K,(p)}$, where n_p is the residue degree of p in K/\mathbb{Q} .*

Let \mathcal{L} be the G -module of relations $U = \sum_{\nu \in G} u(\nu) \nu^{-1} \in \mathbb{Z}_{(p)}[G]$ regarding $\alpha_p(\eta)$, i.e., such that, by definition,

$$\sum_{\nu \in G} u(\nu) \alpha_p(\eta)^{\nu^{-1}} \equiv 0 \pmod{p}, \quad u(\nu) \in \mathbb{Z}_{(p)} \quad (\text{Definitions 3.3}).$$

Let θ be an irreducible p -adic character of G and let f be the residue degree of p in the field of values of the absolutely irreducible characters $\varphi | \theta$.

Then, seen in $\mathbb{F}_p[G]$, the G -module $\mathcal{L}^\theta := e_\theta \mathcal{L}$ is of nonzero \mathbb{F}_p -dimension if and only if the local θ -regulator $\Delta_p^\theta(\eta)$ (§ 2.3) is zero modulo p .

When it is the case, the \mathbb{F}_p -dimension of \mathcal{L}^θ is $\delta f \varphi(1)$, with $1 \leq \delta \leq \varphi(1)$.

Proof. (a) If $\mathcal{L}^\theta \neq \{0\}$, there exists $U = \sum_{\nu \in G} u(\nu) \nu^{-1} \in \mathcal{L}$ such that $U_\theta \not\equiv 0 \pmod{p}$; then $U_\varphi \not\equiv 0 \pmod{\mathfrak{p}}$ for all $\varphi \mid \theta$. From Lemma 3.5 and Corollary 3.6, we have $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$.

(b) Suppose $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$ and let $\alpha \equiv \alpha_p(\eta) \pmod{p}$, $\alpha \in Z_{K,(p)}$; by the resulting nullity modulo p of $\text{Frob}^G(\alpha)$, there exists a relation of \mathbb{F}_p -dependence of the form $\sum_{\nu \in G} u(\nu) \alpha^{\nu^{-1}} \equiv 0 \pmod{p}$, $u(\nu) \in \mathbb{Z}_{(p)}$ not all divisible by p , and we have $U = \sum_{\nu \in G} u(\nu) \nu^{-1} \in \mathcal{L}$ (Corollary 3.2), but we need to deduce that $\mathcal{L}^\theta \neq \{0\}$. From Lemma 3.7, there exists, for $\varphi \mid \theta$, a non trivial φ -relation modulo \mathfrak{p} of the form $W := \sum_{\nu \in G} w(\nu) \nu^{-1}$, $w(\nu) \in Z_{C,(p)}$, such that $W \cdot \alpha \equiv 0 \pmod{\mathfrak{p}}$.

If $\{z, \dots, z^f\}$ is a $Z_{L,(p)}$ -basis of $Z_{C,(p)}$, then $w(\nu) = \sum_{i=1, \dots, f} a_i(\nu) z^i$, with $a_i(\nu) \in Z_{L,(p)}$ for all i and all ν , whence $\sum_{\nu \in G} \sum_{i=1, \dots, f} a_i(\nu) z^i \alpha^{\nu^{-1}} \equiv 0 \pmod{\mathfrak{p}}$; identifying on the basis of the z^i one obtains the system of relations in $Z_{KL,(p)}$

$$\sum_{\nu \in G} a_i(\nu) \alpha^{\nu^{-1}} \equiv 0 \pmod{\mathfrak{p}}, \quad i = 1, \dots, f.$$

For all i , and all ν , there exist some $r_{\mathfrak{p}}^i(\nu) \in \mathbb{Z}$ such that $a_i(\nu) \equiv r_{\mathfrak{p}}^i(\nu) \pmod{\mathfrak{p}}$, whence $\sum_{\nu \in G} a_i(\nu) \alpha^{\nu^{-1}} \equiv \sum_{\nu \in G} r_{\mathfrak{p}}^i(\nu) \alpha^{\nu^{-1}} \equiv 0 \pmod{\mathfrak{p}}$; since $\sum_{\nu \in G} r_{\mathfrak{p}}^i(\nu) \alpha^{\nu^{-1}}$ is in K , this yields $\sum_{\nu \in G} r_{\mathfrak{p}}^i(\nu) \alpha^{\nu^{-1}} \equiv 0 \pmod{p}$. Since W is a non trivial φ -relation modulo \mathfrak{p} , the $r_{\mathfrak{p}}^i(\nu)$ are not all zero modulo p and there exists a non trivial relation $\sum_{\nu \in G} r_{\mathfrak{p}}^i(\nu) \alpha^{\nu^{-1}}$ for at least an index $i \in \{1, \dots, f\}$. As W is a φ -relation, this is transmitted to $\sum_{\nu \in G} a_i(\nu) \alpha^{\nu^{-1}}$ and consequently, $\sum_{\nu \in G} r_{\mathfrak{p}}^i(\nu) \nu^{-1}$ (a φ -relation invariant by D), is a non trivial θ -relation of \mathcal{L} .

In fact one can prove that the matrix $(r_{\mathfrak{p}}^i(\nu))_{i,\nu}$ is of rank f . \square

Corollary 3.10. *When $\mathcal{L}^\theta \neq \{0\}$, we get local lifts of the form $\eta^{U_\theta} \in \prod_{v \mid p} K_v^{\times p}$ for all θ -relation $U_\theta \in \mathcal{L}^\theta$. If we represent, modulo p , $U_\theta \in \mathbb{Z}_p[G]$ by $U'_\theta \in \mathbb{Z}[G]$, then $\eta_1^{U_\theta}$ is a global element of K^\times being a local p th power at p .*

Proof. We have $\eta_1^{U_\theta} = (1 + p \alpha_p(\eta))^{U_\theta} \equiv 1 + p U_\theta \cdot \alpha_p(\eta) \pmod{p^2}$ and, since by definition $U_\theta \cdot \alpha_p(\eta) \equiv 0 \pmod{p}$, this yields $\eta_1^{U_\theta} = 1 + p^2 \beta$, $\beta \in Z_{K,(p)}$. Thus $\eta_1^{U_\theta} = (1 + p \gamma)^p$, $\gamma \in \prod_{v \mid p} K_v$, and $\eta = \eta^{p^{n_p}} \eta_1^{-1}$ implies $\eta^{U_\theta} \in \prod_{v \mid p} K_v^{\times p}$. \square

4. HEURISTIC CONSIDERATIONS AND EXPERIMENTS

4.1. Probabilistic methods. If some events E_p , indexed by the prime numbers, are independent and of probabilities $\text{Pr}(E_p)$, we may apply the heuristic principle of Borel–Cantelli that is to say: if the series $\sum_p \text{Pr}(E_p)$ is convergent, then the natural conjecture is that the events E_p are realized finitely many times, and that if it is divergent they are realized infinitely many times with a suitable density (see [T, Chap. III.1]). In our case, E_p is, for $\eta \in K^\times$ fixed, the events

$$\text{“Reg}_p^G(\eta) \equiv 0 \pmod{p}” \quad \text{or} \quad \text{“}\Delta_p^\theta(\eta) \equiv 0 \pmod{p}”$$

for a choice of θ for each p (§ 2.3). In the general case, since $\text{Reg}_p^\theta(\eta)$ is a local norm in the extension C/\mathbb{Q} , such a local regulator is either prime to p , either divisible by p^f , where f is the residue degree of p in this extension; similarly, if the irreducible character $\varphi | \theta$ is of degree $\varphi(1) \geq 2$, $\text{Reg}_p^G(\eta)$ is divisible by $p^{f\varphi(1)}$.

We shall see that the degree $\varphi(1)$ does not occur for probabilities but that, on the contrary, the number δ such that $\mathcal{L}^\theta \simeq \delta V_\theta$ occurs, as well as f , under the formula $\frac{O(1)}{p^{f\delta^2}}$ which is the probability to have “ $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$ & $\mathcal{L}^\theta \simeq \delta V_\theta$ ” (§ 4.2.2).

We shall neglect primes p for which at least two θ -regulators $\Delta_p^\theta(\eta)$ are divisible by p , such a probability being at most $\frac{O(1)}{p^2}$, given the independence of the local θ -regulators (§ 4.3).

It will remain the case $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$ for a unique p -adic character θ of G under the conditions $f = 1$ and the representation \mathcal{L}^θ being minimal (i.e., $\delta = 1$); then we will have $\text{Reg}_p^G(\eta) \sim p^{e\varphi(1)}$ with $e = 1$, the case $e \geq 2$ being also of probability at most $\frac{O(1)}{p^2}$ (§ 4.6).

The obstruction for the utilisation of the heuristic principle of Borel–Cantelli would come from primes p satisfying the following definition:

Definition 4.1. A prime number p constitutes a case of *minimal p -divisibility* for the normalized regulator $\text{Reg}_p^G(\eta)$ if $\mathcal{L}^\theta \neq 0$ (i.e., $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$) for a unique irreducible p -adic character θ of G satisfying furthermore the following conditions

- (i) p is totally split in C (i.e., $f = 1$),
- (ii) $\mathcal{L}^\theta \simeq V_\theta$ (i.e., $\delta = 1$),
- (iii) $\text{Reg}_p^\theta(\eta) \sim p$ (i.e., $\text{Reg}_p^G(\eta) \sim p^{\varphi(1)}$ has no extra p -divisibilities).

If G is Abelian, this concerns certain $p \equiv 1 \pmod{d}$, where d is the order of $\varphi | \theta$.

If $G = 1$ (situation of the Fermat quotient of a rational), this occurs for all p .

4.2. Principles of analysis – linearization of the problem. Let $\eta \in Z_K$ be given such that the multiplicative G -module generated by η is of \mathbb{Z} -rank n , even if any case of sub-representation may be studied in an analogous way.

4.2.1. Densities vs probabilities. We can verify by experiments the following heuristic principles using the function *random* of PARI to define an arbitrary integer γ of K , prime to p (in fact we are only interested by the class modulo p^2 of γ):

- (i) If under a p -adic point of view, $\alpha_p(\gamma) \pmod{p}$ runs through the quotient ring $Z_{K,(p)}/(p) \simeq \mathbb{F}_p^n$, experiments show that the statistical result remains excellent if one limits γ into a small *Archimedean* domain (defined for instance by $|c_i| \ll p$ for the components c_i of γ on a basis, or by $\max_{\nu \in G}(|\gamma^\nu|) \ll p$), which preserves the Diophantine aspect and proves an uniform distribution (required limitation when p^n is very large). In [H-B] it is proved the uniform distribution of Fermat quotients and it is easy to conjecture that this is general.

As explained in Remark 2.4, we must distinguish the notion of probability (γ fixed and $p \rightarrow \infty$) from that of density, purely algebraic, when they are equal to $\frac{O(1)}{p}$; we establish Sections 6 and 7 the analogue of the study conducted in [Gr2] for Fermat quotients (with numerical verifications for the groups C_3, D_6), which constitutes a serious justification of the conjectures of Section 8.

(ii) Let $(e_i)_{i=1,\dots,n}$ be a $\mathbb{Z}_{(p)}$ -basis of $Z_{K,(p)}$ and put $\alpha_p(\gamma) = \sum_{i=1}^n A_i e_i$, $A_i \in \mathbb{Z}_{(p)}$; then, modulo p , the variables A_i are independent and equiprobable in \mathbb{F}_p , and this does not depend on K nor of the choice of the basis.

Any non trivial relation of the form $\sum_{\nu \in G} u(\nu) \alpha_p(\gamma)^{\nu-1} \equiv 0 \pmod{p}$ is translated into an analogous non trivial relation on the A_i (because the conjugates of the e_j are linear forms on the e_i , independent of p).

4.2.2. Main Heuristic. The probability (comming from the corresponding density) of $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$ is that of $\mathcal{L}^\theta \neq \{0\}$ (Definitions 3.3, Theorem 3.9). If $\mathcal{L}^\theta \simeq \delta V_\theta$, $\delta \neq 0$, we shall justify that we must assign to this case the probability

$$\text{Prob}\left(\mathcal{L}^\theta \simeq \delta V_\theta, 1 \leq \delta \leq \varphi(1)\right) \leq \frac{O(1)}{p^f \delta^2},$$

where f is the residue degree of θ , where we consider V_θ as a \mathbb{F}_p -representation and then, by extension of scalars, $V_\theta \otimes \mathbb{F}_{p^f}$ and V_φ as \mathbb{F}_{p^f} -representations.

Indeed, we have $\mathcal{L}^\theta \otimes \mathbb{F}_{p^f} = \bigoplus_{\varphi|\theta} \mathcal{L}^\varphi$, where $\mathcal{L}^\varphi \simeq \delta V_\varphi$, and the idea comes from the fact that when $\mathcal{L}^\varphi \simeq \varphi(1)V_\varphi \simeq e_\varphi \mathbb{F}_{p^f}[G]$ (i.e., $e_\varphi \alpha_p(\eta) \equiv 0 \pmod{p}$), the correspondent probability is $\frac{O(1)}{p^f \varphi(1)^2}$ (minimal) since $e_\varphi \alpha_p(\eta)$ is defined by $f\varphi(1)^2$ \mathbb{F}_p -independent components (\mathbb{F}_p -dimension of $\varphi(1)V_\varphi$). But $e_\varphi \mathbb{F}_{p^f}[G] \simeq \text{End}(V_\varphi)$ as an algebra of endomorphisms of a \mathbb{F}_{p^f} -space of dimension $\varphi(1)$.

Therefore, $\mathcal{L}^\varphi \simeq \delta V_\varphi$ is then seen as a sub-algebra of endomorphisms of a \mathbb{F}_{p^f} -space of dimension δ , whence a probability-density $\frac{O(1)}{p^f \delta^2}$ to get $\mathcal{L}^\varphi \simeq \delta V_\varphi$ (i.e., $\mathcal{L}^\theta \simeq \delta V_\theta$). The case $f = \delta = 1$ establishes the case where the notion of probability must be substituted for that of density.

We shall note that the probability to have all the $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$ with each time $\delta = \varphi(1)$ (i.e., $\alpha_p(\eta) \equiv 0 \pmod{p}$), equivalent for the n components of $\alpha_p(\eta)$ to be zero modulo p is then $\frac{O(1)}{p^n}$ since $\sum_\theta f\varphi(1)^2 = |G| = n$. This shows the consistency of the proposed heuristic.

The most frequent non trivial case is $\delta = 1$ (the residue degree f depends canonically of p contrary to δ which is “numerical”). For instance, from $\delta = 1$ to $\delta = 2$ (for $f = 1$), this increases the probabilities from $\frac{O(1)}{p}$ to $\frac{O(1)}{p^4}$, near from zero for $p \rightarrow \infty$ (very well confirmed by numerical statistics, cf. § 4.4.3).

Example 4.2. Case of $G = D_6$ ($f = 1$, $1 \leq \delta \leq 2$). Let θ be the irreducible character of degree 2; the representation $e_\theta \mathbb{F}_p[G]$ is isomorphic to $2V_\theta$ where V_θ is of \mathbb{F}_p -dimension 2. On may generate $e_\theta \mathbb{F}_p[G]$ as follows (see Remark 2.13 (ii))

$$\begin{aligned} U_1 &= 1 - \sigma^2 + \tau - \tau\sigma, & \sigma U_1 &= \sigma - 1 + \tau\sigma^2 - \tau, & \sigma^2 U_1 &= -U_1 - \sigma U_1, \\ U_2 &= 1 - \sigma - \tau + \tau\sigma, & \sigma U_2 &= -\sigma^2 + \sigma + \tau - \tau\sigma^2, & \sigma^2 U_2 &= -U_2 - \sigma U_2, \\ \tau U_1 &= -\sigma U_1, & \tau\sigma U_1 &= -U_1, & \tau\sigma^2 U_1 &= -\sigma^2 U_1, \\ \tau U_2 &= -U_2, & \tau\sigma U_2 &= -\sigma^2 U_2, & \tau\sigma^2 U_2 &= -\sigma U_2. \end{aligned}$$

The elements $U_1, \sigma U_1, U_2, \sigma U_2$ constitute a \mathbb{F}_p -basis of the space of the θ -relations, which justifies the probability $\frac{O(1)}{p}$ only for the case $\delta = 1$, but $\frac{O(1)}{p^4}$ for $\delta = 2$.

4.3. Probabilistic independence (over θ) of the variables $\Delta_p^\theta(\gamma)$. We process the case of the group D_6 , by use of the *random* function, to verify two aspects:

- (i) The independence of the θ -regulators (probability at most $\frac{O(1)}{p^2}$ to get two θ -regulators $\Delta_p^\theta(\gamma)$ and $\Delta_p^{\theta'}(\gamma)$ null modulo p , for $\theta \neq \theta'$).
- (ii) the probability $\frac{O(1)}{p}$ to have the nullity modulo p of $\Delta_p^\theta(\gamma)$ for the character $\theta = \chi_2$ of degree 2, the case of characters of degree 1 being analogous.

We consider the field K (compositum of $\mathbb{Q}(\sqrt[3]{2})$ and of $\mathbb{Q}(j)$, where j denotes a cubic root of unity) defined by the polynomial

$$Q = x^6 + 9x^4 - 4x^3 + 27x^2 + 36x + 31.$$

We take at random γ modulo p^2 , prime to p , which gives some $\alpha = \alpha_p(\gamma)$ uniformly distributed modulo p . The Pr. A-3 of [Gr4] compute the conjugates of α on the basis $\{x^5, x^4, x^3, x^2, x, 1\}$. The variable N_0 is the number of γ prime to p . The variables $N_1, N_2, N_3, N_{12}, N_{13}, N_{23}, N_{123}$ give the number of cases of simultaneous nullities of 1, 2 or 3 regulators (characters χ_0, χ_1, χ_2 of degree 2, respectively).

For $p = 13$ we obtain the following values

$$\begin{aligned} N_0 &= 999115 ; N_1 = 76820 ; N_2 = 77009 ; N_3 = 82239 ; \\ N_{12} &= 5898 ; N_{13} = 6301 ; N_{23} = 6453 ; N_{123} = 442, \text{ and the respective densities} \\ \frac{N_1}{N_0} &= 0.076888 ; \frac{N_2}{N_0} = 0.07707 ; \frac{N_3}{N_0} = 0.0823 ; \\ \frac{N_{12}}{N_0} &= 0.00590 ; \frac{N_{13}}{N_0} = 0.006306 ; \frac{N_{23}}{N_0} = 0.006458 ; \frac{N_{123}}{N_0} = 0.0004424 ; \\ \text{with } \frac{1}{p} &= 0.07692, \frac{1}{p^2} = 0.005917, \frac{1}{p^3} = 0.000455, \text{ whence the expected probabilities.} \end{aligned}$$

For $p = 37$ we obtain the following values

$$\begin{aligned} N_0 &= 999952 ; N_1 = 27153 ; N_2 = 27054 ; N_3 = 27747 ; \\ N_{12} &= 718 ; N_{13} = 761 ; N_{23} = 755 ; N_{123} = 16, \text{ and the respective densities} \\ \frac{N_1}{N_0} &= 0.0271543 ; \frac{N_2}{N_0} = 0.027055 ; \frac{N_3}{N_0} = 0.0277483 ; \\ \frac{N_{12}}{N_0} &= 0.000718 ; \frac{N_{13}}{N_0} = 0.000761 ; \frac{N_{23}}{N_0} = 0.000755 ; \frac{N_{123}}{N_0} = 1.600 \times 10^{-5}, \\ \text{with } \frac{1}{p} &= 0.027027, \frac{1}{p^2} = 0.00073046, \frac{1}{p^3} = 1.97 \times 10^{-5}. \end{aligned}$$

4.4. Statistics on the matrix rank of the components. A first statistic experiment consists in determining the probability to have at least a non trivial relation between the conjugates of α ; if $\alpha^\nu = \sum_{i=1}^n A_i(\nu) e_i$, then the matrix $(A_i(\nu))_{i,\nu}$ must be of \mathbb{F}_p -rank strictly less than n . For $\theta | \chi$, the probability of nullity modulo p of a single $\Delta_p^\theta(\gamma)$ is $\frac{1}{p^{f\delta^2}}$; the probability to have at least a $\Delta_p^\theta(\gamma)$ zero modulo p for $\theta | \chi$ is $\frac{h}{p^{f\delta^2}}$. So if we denote by h_i, f_i, δ_i , the above parameters for the totality of the p -adic characters of G (grouped by rational characters χ_i), the theoretical probability to obtain a matrix of \mathbb{F}_p -rank $< n$ is given by

$$\sum_i \frac{h_i}{p^{f_i\delta_i^2}} - \sum_{i < j} \frac{h_i}{p^{f_i\delta_i^2}} \frac{h_j}{p^{f_j\delta_j^2}} + \sum_{i < j < k} \frac{h_i}{p^{f_i\delta_i^2}} \frac{h_j}{p^{f_j\delta_j^2}} \frac{h_k}{p^{f_k\delta_k^2}} - \dots,$$

which can be verified by means of programs calculating, for some random γ , the number of cases of \mathbb{F}_p -rank $< n$ ($G \simeq C_3, C_5, D_6$, respectively, in the variables

N_3, N_5, N_6). Each group G is given via a polynomial defining K , but numerical experiments show that the nature of the probabilistic results only depends on G but not of the choice of K nor of the polynomial defining it.

4.4.1. *Case G cyclic of order 3* (two rational characters). We use the Shanks polynomial $P = x^3 - 11x^2 - 14x - 1$. In the case $p \equiv 1 \pmod{3}$ we have three p -adic characters of residue degree $f = 1$, in the case $p \equiv 2 \pmod{3}$ we have a p -adic character of residue degree $f = 2$ and the unit character. We obtain the following examples (see [Gr4, Pr. A-4]), where N_0 is the number of tested cases

$$p = 41, N_0 = 4999931, N_3 = 124889, \frac{N_3}{N_0} = 0.024978, \text{probability } 0.024970.$$

$$p = 43, N_0 = 4999952, N_3 = 341000, \frac{N_3}{N_0} = 0.068200, \text{probability } 0.068685.$$

4.4.2. *Case G cyclic of order 5* (two rational characters). It is the unique studied case for which there are (for $p \equiv -1 \pmod{5}$) two p -adic characters of residue degree $f = 2$. Numerical values obtained (see [Gr4, Pr. A-5.1]):

$$p = 7, N_0 = 499977, N_5 = 71650, \frac{N_5}{N_0} = 0.14330, \text{probability } 0.143214.$$

$$p = 19, N_0 = 500000, N_5 = 29033, \frac{N_5}{N_0} = 0.05806, \text{probability } 0.057880.$$

$$p = 31, N_0 = 500000, N_5 = 75737, \frac{N_5}{N_0} = 0.15147, \text{probability } 0.151214.$$

By modification of the end of the program ([Gr4, Pr. A-5.2]), we test the frequency of nullity modulo p of the θ -regulators related to two p -adic characters ($p = 31$ totally split), and only two among the four non trivial characters, namely for instance for θ_1 and θ_2 defined by $\theta_1(\sigma^{-1}) \equiv 2, \theta_2(\sigma^{-1}) \equiv 4 \pmod{p}$

$$\Delta_p^{\theta_1}(\gamma) = \alpha + 2\alpha^\sigma + 4\alpha^{\sigma^2} + 8\alpha^{\sigma^3} + 16\alpha^{\sigma^4},$$

$$\Delta_p^{\theta_2}(\gamma) = \alpha + 4\alpha^\sigma + 16\alpha^{\sigma^2} + 2\alpha^{\sigma^3} + 8\alpha^{\sigma^4}.$$

For $N_0 = 1000000, N_1 = 943$ (number of simultaneous nullities of the two regulators), we have $\frac{N_1}{N_0} = 0.000943$ and the probability 0.001040, which shows the independence of regulators regarding the p -adic characters of a same rational character.

4.4.3. *Case G dihedral of order 6* (three rational and p -adic characters). In this case we have $h = f = 1$ for all the characters. The results do not depend on congruence classes of the primes p because $C = \mathbb{Q}$ (see [Gr4, Pr. A-6.1]):

$$p = 13, N_0 = 49954, N_6 = 10794, \frac{N_6}{N_0} = 0.21607, \text{probability } 0.21347.$$

$$p = 17, N_0 = 49516, N_6 = 8337, \frac{N_6}{N_0} = 0.16836, \text{probability } 0.16629.$$

$$p = 29, N_0 = 49815, N_6 = 5056, \frac{N_6}{N_0} = 0.10149, \text{probability } 0.09992.$$

$$p = 31, N_0 = 40982, N_6 = 3854, \frac{N_6}{N_0} = 0.09404, \text{probability } 0.09368.$$

$$p = 37, N_0 = 49998, N_6 = 3959, \frac{N_6}{N_0} = 0.07918, \text{probability } 0.07890.$$

Then we take again the same program to make the statistics of the case $\delta = 2$ for the character χ_2 of degree 2, which may be tested by computing the number N_2 of cases where the regulators $\Delta_p^1(\gamma)$ and $\Delta_p^{\chi_1}(\gamma)$ are nonzero modulo p , and the matrix of the components of rank 2. This is equivalent to

$$\Delta_p^\theta(\gamma) \equiv 0 \pmod{p} \text{ for } \theta = \chi_2 \text{ and } \mathcal{L}^\theta \text{ of dimension } 4$$

([Gr4, Pr. A-6.2]). We get the following result for $p = 13$

$$N_0 = 499541; N_2 = 18; \frac{N_2}{N_0} = 3.60 \times 10^{-5}; \frac{1}{p^4} = 3.50 \times 10^{-5};$$

$N_1 = 34925$ (number of $\Delta_p^{\chi_2}(\gamma) \equiv 0 \pmod{p}$); $\frac{N_1}{N_0} = 0.06991$; $\frac{1}{p} = 0.07692$.

4.5. Local independence of the components on a basis. It remains to verify the nature of “independent random variables” of A_1, \dots, A_n ; we only give two numerical examples ($G = C_3$ and $G = D_6$).

4.5.1. Cubique cyclic case. Let K be the cubic cyclic field defined by the polynomial $x^3 - 11x^2 - 14x - 1$, of conductor 163. This is to check that the variables A, B, C , defining $\alpha \equiv Ax^2 + Bx + C \pmod{p}$ are independent.

The Pr. A-7 of [Gr4] considers random prime to p integers γ modulo p^2 , in a small sub-domain of $(\mathbb{Z}/p^2\mathbb{Z})^3$. Then it computes for instance the number of pairs (A, B) (resp. (B, C) , (C, A)) having an arbitrary fixed value in \mathbb{F}_p^2 , then the number of cases where $\Delta_p^{\chi}(\gamma) \equiv 0 \pmod{p}$.

We denote by N_0 the number of prime to p integers γ modulo p^2 considered, by N_1 the number of cases where $\Delta_p^{\chi}(\gamma) \equiv 0 \pmod{p}$ (χ rational $\neq 1$), by N_2 the number of pairs (A, B) having the imposed value modulo p , and the program computes the proportions $\frac{N_1}{N_0}$, $\frac{N_2}{N_0}$, together with $\frac{2}{p}$ or $\frac{1}{p^2}$.

In the array below, we give two cases of residue degree 2 in $\mathbb{Q}(j)/\mathbb{Q}$ ($j^3 = 1, j \neq 1$) and we continue with totally split cases

p	N_0	N_1	N_2	$\frac{N_1}{N_0}$	$\frac{N_2}{N_0}$	$\frac{1}{p^2}$	
5	255562	10023	10155	0.039219	0.039736	0.04	
11	499624	4127	4191	0.00826	0.008388	0.00826	
p	N_0	N_1	N_2	$\frac{N_1}{N_0}$	$\frac{N_2}{N_0}$	$\frac{1}{p^2}$	$\frac{2}{p}$
7	498553	132167	10275	0.2651	0.0206	0.0204	0.286
13	392751	57826	2401	0.1472	0.006113	0.005917	0.154
19	499907	51293	1421	0.1025	0.00284	0.00277	0.105

The proportions $\frac{N_2}{N_0}$ are near from $\frac{1}{p^2}$. In all the cases $p \equiv 1 \pmod{3}$ the proportions $\frac{N_1}{N_0}$ are near from $\frac{2}{p}$ (existence of two p -adic characters), and near from $\frac{1}{p^2}$ in the case $p \equiv 2 \pmod{3}$. If we only impose a numerical value, one gets a proportion near from $\frac{1}{p}$, and near from $\frac{1}{p^3}$ if we impose the three values.

4.5.2. Dihedral case D_6 . An analogous study uses Pr. A-8 of [Gr4] and gives the expected results. For $p = 17$, we obtain for three conditions among the six components of α , $N_0 = 494865$, $N_3 = 111$ and $\frac{N_3}{N_0} = 0.0002243$, for $\frac{1}{p^3} = 0.0002035$.

4.6. Extra p -divisibilities of regulators. Recall the decomposition of the normalized regulator of η (Remark 2.10 and § 2.3.2)

$$\text{Reg}_p^G(\eta) = \prod_{\theta} \text{Reg}_p^{\theta}(\eta)^{\varphi(1)} \text{ and } \text{Reg}_p^{\theta}(\eta) = N_p(P^{\varphi}(\dots, \frac{-1}{p}\log_p(\eta^{\nu}), \dots)).$$

In the case of minimal p -divisibility (Definition 4.1), we have $\text{Reg}_p^{\theta}(\eta) \sim p$ for a unique θ , and $\text{Reg}_p^G(\eta) \sim p^{\varphi(1)}$.

If we only suppose that p is totally split in C/\mathbb{Q} ($f = 1$) and that there exists θ such that $\text{Reg}_p^{\theta}(\eta) \equiv \Delta_p^{\theta}(\eta) \equiv 0 \pmod{p}$ (with $\delta = 1$), we may have possible extra p -divisibilities $\text{Reg}_p^{\theta}(\eta) \sim p^e$, $e \geq 2$ (then $\text{Reg}_p^G(\eta) \sim p^{e\varphi(1)}$ if θ is unique), for which we want to verify that they are of probability $\frac{O(1)}{p^2}$.

In [Gr4], for $K = \mathbb{Q}(j, \sqrt[3]{2})$, $G = D_6$ (in which case any large enough p is convenient for the test), the Pr. A-9 checks this fact for the regulator

$$\text{Reg}_p^{\chi_2}(\eta) = \frac{1}{\sqrt{-3}}(E_1^2 + E_2^2 + E_3^2 - E_4^2 - E_5^2 - E_6^2 - E_1.E_2 - E_2.E_3 - E_3.E_1 \\ + E_4.E_5 + E_5.E_6 + E_6.E_4) \in \mathbb{Z},$$

where the E_i , $1 \leq i \leq 6$, are the conjugates of an integer of K (indeed, one may suppose that $\frac{-1}{p}\log_p(\eta)$ is represented modulo p^2 by an arbitrary integer $E \in K$).

For $p = 101$ and 10^6 tests via *random*, we obtain a density of cases $e \geq 2$ equal to 1.01×10^{-4} for a theoretical probability 0.98×10^{-4} .

For $p = 149$, we obtain 4.60×10^{-5} for a probability 4.50×10^{-5} .

The case of characters of degree 1 offers no difficulty (under the condition $f = 1$) and we shall make the heuristic assumption that it is the same for all group and all character in the p -splitted case, and in particular that $P^\varphi(\dots, \frac{-1}{p}\log_p(\eta^\nu), \dots)$ may have any p -adic valuation with the corresponding probability. It would be interesting to prove that this property of the polynomials $P^\varphi(X)$ is universal.

5. NUMERICAL STUDY OF TWO PARTICULAR CASES

5.1. Abelian case. We can always reduce to the case where G is cyclic of order $n > 2$, generated by σ (see § 2.3.3 for the case $n \leq 2$).

5.1.1. Example of the maximal real subfield of $\mathbb{Q}(\mu_{11})$.

a) Search of solutions p such that $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$. Put

$$\eta = ax^4 + bx^3 + cx^2 + dx + e, \text{ with } x = \zeta_{11} + \zeta_{11}^{-1}$$

(see [Gr4, Pr. A-11 and A-10 for the cubic case],).

(i) For $\eta = -2x^4 + x^3 - 3$, the solutions $p \leq 10^7$ are 31, 101, 39451 splitted in $\mathbb{Q}(\zeta_5)$.

Consider the numerical data for $p = 31$

$$\begin{aligned} \alpha &\equiv 25x^4 + 10x^3 + 7x^2 + 21x + 29 \pmod{p} \\ \alpha^\sigma &\equiv 4x^4 + 15x^3 + 25x^2 + 7x + 16 \pmod{p} \\ \alpha^{\sigma^2} &\equiv 26x^4 + 20x^3 + 26x^2 + 18x + 22 \pmod{p} \\ \alpha^{\sigma^3} &\equiv 17x^4 + 6x^3 + 21x^2 + 24x + 4 \pmod{p} \\ \alpha^{\sigma^4} &\equiv 21x^4 + 11x^3 + 14x^2 + 23x + 19 \pmod{p} \end{aligned}$$

For $r = 4$, which is such that $\theta(\sigma) \equiv r \pmod{\mathfrak{p}}$ for a pair (θ, \mathfrak{p}) , we immediately have, as expected

$$\Delta_p^\theta(\eta) = \alpha + r^{-1}\alpha^\sigma + r^{-2}\alpha^{\sigma^2} + r^{-3}\alpha^{\sigma^3} + r^{-4}\alpha^{\sigma^4} \equiv 0 \pmod{p}$$

identically on the basis $\{x^4, x^3, x^2, x, 1\}$.

(ii) For $\eta = 10x^4 - 7x^3 + x - 2$, we find the unique solution $p = 7$, first totally inert case in $\mathbb{Q}(\zeta_5)$. The program gives that all the conjugates of α are zero modulo p (whence moreover $\Delta_p^1(\eta) \equiv 0 \pmod{p}$).

It is clear that the inert case in $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ is very rare. Furthermore, p is small to compensate a probability $\frac{O(1)}{p^4}$.

(iii) For $\eta = 10x^4 - 7x^3 - 3x^2 + x - 2$, we find $p = 79$ (two p -adic characters θ of residue degree $f = 2$; p splitted in $L = \mathbb{Q}(\sqrt{5})$).

The resolvent $\alpha + \zeta_5 \alpha^\sigma + \zeta_5^2 \alpha^{\sigma^2} + \zeta_5^3 \alpha^{\sigma^3} + \zeta_5^4 \alpha^{\sigma^4}$ (which corresponds to $\Delta_p^\varphi(\eta)$ for $\varphi(\sigma) = \zeta_5^{-1}$) is decomposed in the following way on the relativ basis $\{1, \zeta_5\}$.

We have the relation $\zeta_5^2 - \zeta_5 \frac{\sqrt{5}-1}{2} + 1 = 0$ defining the irreducible polynomial of ζ_5 over $\mathbb{Q}(\sqrt{5})$. We then get $\zeta_5^3 = -\zeta_5 \frac{\sqrt{5}-1}{2} + \frac{1-\sqrt{5}}{2}$, $\zeta_5^4 = -\zeta_5 + \frac{\sqrt{5}-1}{2}$, and the system of relations in $K(\zeta_5)$ expressing $\Delta_p^\varphi(\eta) \equiv 0 \pmod{\mathfrak{p}}$

$$\begin{aligned} \alpha - \alpha^{\sigma^2} + \frac{\sqrt{5}-1}{2}(\alpha^{\sigma^4} - \alpha^{\sigma^3}) &\equiv 0 \pmod{\mathfrak{p}} \\ \alpha^\sigma - \alpha^{\sigma^4} + \frac{\sqrt{5}-1}{2}(\alpha^{\sigma^2} - \alpha^{\sigma^3}) &\equiv 0 \pmod{\mathfrak{p}}. \end{aligned}$$

Then, the ideal \mathfrak{p} is for instance defined by the congruence $\sqrt{5} \equiv 20 \pmod{\mathfrak{p}}$, whence $\frac{\sqrt{5}-1}{2} \equiv 49 \pmod{\mathfrak{p}}$ which defines the coefficients $r_i(\nu)$, $i = 1, 2$, and (θ, \mathfrak{p}) .

We have obtained two linear relations with independent rational coefficients

$$\begin{aligned} \alpha - \alpha^{\sigma^2} + 49(\alpha^{\sigma^4} - \alpha^{\sigma^3}) &\equiv 0 \pmod{p} \\ \alpha^{\sigma^4} - \alpha^\sigma + 49(\alpha^{\sigma^3} - \alpha^{\sigma^2}) &\equiv 0 \pmod{p}. \end{aligned}$$

The numerical data for α and its conjugates are

$$\begin{aligned} \alpha &\equiv 37x^4 + 13x^3 + 19x^2 + 3x + 10 \pmod{p} \\ \alpha^\sigma &\equiv 75x^4 + 24x^3 + 45x^2 + 73x + 33 \pmod{p} \\ \alpha^{\sigma^2} &\equiv 5x^4 + 51x^3 + 22x^2 + 60x + 1 \pmod{p} \\ \alpha^{\sigma^3} &\equiv 70x^4 + 33x^3 + 40x^2 + 8x + 77 \pmod{p} \\ \alpha^{\sigma^4} &\equiv 50x^4 + 37x^3 + 32x^2 + 14x + 22 \pmod{p} \end{aligned}$$

which satisfy the system of the two above congruences.

We have the two independent relations, defining $\mathcal{L}^\theta \simeq V_\theta$ of \mathbb{F}_p -dimension 2

$$1 - \sigma^2 + 49(\sigma^4 - \sigma^3) \quad \& \quad \sigma^4 - \sigma + 49(\sigma^3 - \sigma^2),$$

the second one being the conjugate by σ^4 of the first one. Whence the probability $\frac{2}{p^2}$ (two choices $\sqrt{5} \equiv \pm 20 \pmod{\mathfrak{p}}$).

b) Computation of the density of $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$ as a function of f . In [Gr4, Pr. A-12], the program takes again the previous case and is concerned with the various possible residue degrees of p in $\mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})/\mathbb{Q}$ to verify that the probability for $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$ is indeed $\frac{O(1)}{p^f}$.

We display the theoretical probabilities, depending on the case ($f = 1, 2, 4$), and the number N_1 of solutions compared with the number N_0 of tested η .

For $p = 31$, the residue degree is 1 and we obtain the values $N_1 = 61505$, $\frac{N_1}{N_0} = 0.1230$ for $\frac{4}{p} - \frac{6}{p^2} + \frac{4}{p^3} - \frac{1}{p^4} = 0.12292$.

For $p = 19$, the residue degree is 2 and we obtain the values $N_1 = 2756$, $\frac{N_1}{N_0} = 0.005512$ for $\frac{2}{p^2} - \frac{1}{p^4} = 0.00553$.

For $p = 13$, the residue degree is 4 and we obtain the values $N_1 = 17$, $\frac{N_1}{N_0} = 3.40 \times 10^{-5}$ for $\frac{1}{p^4} = 3.50 \times 10^{-5}$.

5.2. Case of the group D_6 . Let $k = \mathbb{Q}(\sqrt{m})$ be the quadratic subfield of K and let χ_1, χ_2 be the two non trivial irreducible rational characters (and p -adic) of D_6 . We still use $K = \mathbb{Q}(\sqrt[3]{2}, j)$ where j denotes a cubic root of unity ($m = -3$).

5.2.1. *Recalls.* We study the three local χ -regulators $\Delta_p^\chi(\eta)$, each time supposed non trivially null modulo p (no χ -relations in F). We have

$$\alpha = \alpha_p(\eta), \alpha' = \alpha^\sigma, \alpha'' = \alpha^{\sigma^2}, \beta = \alpha^\tau, \beta' = \alpha^{\tau\sigma} = \alpha'^\tau, \beta'' = \alpha^{\tau\sigma^2} = \alpha''^\tau.$$

(i) Case of $\Delta_p^1(\eta)$; thus $N_{K/\mathbb{Q}}(\eta) = a \neq \pm 1$, in which case, $\Delta_p^1(\eta)$ is the Fermat quotient of a .

(ii) Cas $\Delta_p^{\chi_1}(\eta)$; thus $N_{K/k}(\eta) \in k^\times \setminus \mathbb{Q}^\times$ and we suppose that

$$\Delta_p^{\chi_1}(\eta) = \alpha + \alpha' + \alpha'' - \beta - \beta' - \beta'' \equiv 0 \pmod{p}.$$

If $A = \alpha + \alpha' + \alpha'' =: u + v\sqrt{m}$, then $\Delta_p^{\chi_1}(\eta) = A - A^\tau = 2v\sqrt{m} \equiv 0 \pmod{p}$; we then have the unique condition $v \equiv 0 \pmod{p}$, which yields the probability $\frac{O(1)}{p}$.

(iii) Case $\Delta_p^{\chi_2}(\eta)$ (considered up to the factor \sqrt{m}); we have $\dim((F \otimes \mathbb{Q})^{\epsilon_\chi}) = 4$ (case of a character of degree 2), which yields, for $\varphi = \theta = \chi_2$, the condition

$$\begin{aligned} \Delta_p^\theta(\eta) &= \alpha^2 + \alpha'^2 + \alpha''^2 - \beta^2 - \beta'^2 - \beta''^2 \\ &\quad - \alpha\alpha' - \alpha'\alpha'' - \alpha''\alpha + \beta\beta' + \beta'\beta'' + \beta''\beta \equiv 0 \pmod{p} \end{aligned}$$

(cf. Example 2.8). The calculation of the three representations

$$\mathcal{L}^{\theta'} \simeq \delta' V_{\theta'}, \quad 0 \leq \delta' \leq \varphi'(1),$$

allows us to know what are the $\Delta_p^{\theta'}(\eta)$ equal to zero modulo p , even if we can exclude the case where $\Delta_p^1(\eta)$ or $\Delta_p^{\chi_1}(\eta)$ is zero modulo p .

We begin with examples concerning the p -adic character $\theta = \chi_2$. The Pr. A-13 of [Gr4] computes the conjugates of α on the basis of powers of $x = \sqrt[3]{2} + j$. This allows us to find the relations of \mathbb{F}_p -dependence of these conjugates, under the form

$$c_1\alpha + c_2\alpha^\sigma + c_3\alpha^{\sigma^2} + c_4\alpha^\tau + c_5\alpha^{\tau\sigma} + c_6\alpha^{\tau\sigma^2} \equiv 0 \pmod{p}.$$

5.2.2. *Case $\eta = x^5 - 3x^4 - 7x^2 + x - 1$.* We find the solutions $p = 7, 13, 69677, 387161$, up to 10^7 .

a) For $p = 7$, we have the following numerical data

$$\begin{aligned} \alpha &\equiv 0x^5 + 2x^4 + 1x^3 + 1x^2 + 5x + 0 \pmod{p} \\ \alpha^\sigma &\equiv 1x^5 + 1x^4 + 6x^3 + 3x^2 + 5x + 2 \pmod{p} \\ \alpha^{\sigma^2} &\equiv 0x^5 + 2x^4 + 3x^3 + 0x^2 + 4x + 0 \pmod{p} \\ \alpha^\tau &\equiv 0x^5 + 5x^4 + 6x^3 + 6x^2 + 2x + 6 \pmod{p} \\ \alpha^{\tau\sigma} &\equiv 0x^5 + 5x^4 + 4x^3 + 0x^2 + 3x + 6 \pmod{p} \\ \alpha^{\tau\sigma^2} &\equiv 6x^5 + 6x^4 + 1x^3 + 4x^2 + 2x + 4 \pmod{p}, \end{aligned}$$

which yields the two linearly independent \mathbb{F}_p -relations

$$\alpha - \alpha^\sigma + \alpha^\tau - \alpha^{\tau\sigma^2} \equiv 0 \pmod{p} \quad \& \quad \alpha - \alpha^{\sigma^2} + \alpha^\tau - \alpha^{\tau\sigma} \equiv 0 \pmod{p},$$

and their lifts

$$\eta_1^{1-\sigma+\tau-\tau\sigma^2} \equiv 1 \pmod{p^2} \quad \& \quad \eta_1^{1-\sigma^2+\tau-\tau\sigma} \equiv 1 \pmod{p^2}.$$

For the θ -relation $U = 1 - \sigma + \tau - \tau\sigma^2$ we obtain $\sigma^2 U = -U - \sigma U$, $\tau U = -\sigma^2 U$, $\tau\sigma U = -\sigma U$, $\tau\sigma^2 U = -U$, and U generates a space of dimension 2 ($\mathcal{L}^\theta \simeq V_\theta$).

b) For $p = 13$, we obtain the relations

$$\alpha - \alpha^{\sigma^2} + \alpha^\tau - \alpha^{\tau\sigma^2} \equiv 0 \pmod{p} \quad \& \quad \alpha^{\sigma^2} - \alpha^\sigma + \alpha^{\tau\sigma} - \alpha^\tau \equiv 0 \pmod{p}$$

and their lifts

$$\eta_1^{1-\sigma^2+\tau-\tau\sigma^2} \equiv 1 \pmod{p^2} \quad \& \quad \eta_1^{\sigma^2-\sigma+\tau\sigma-\tau} \equiv 1 \pmod{p^2}.$$

For the θ -relation $U = 1 - \sigma^2 + \tau - \tau\sigma^2$, we obtain $\sigma^2 U = -U - \sigma U$, $\tau U = U$, $\tau\sigma U = \sigma^2 U$, $\tau\sigma^2 = \sigma U$ ($\mathcal{L}^\theta \simeq V_\theta$).

c) In the case of $p = 69677$, we find the coefficients $(c_1, c_2, c_3, c_4, c_5, c_6) = (53404, 39540, 46410, 69676, 1, 0)$ & $(23267, 16273, 30137, 69676, 0, 1)$ and a similar conclusion.

5.2.3. *Case $\eta = x^5 - x^4 - 7x^2 + x - 1$, $p = 7$.* We obtain four independent \mathbb{F}_p -linear relations as

$$\alpha^\tau - \alpha \equiv 0 \pmod{p} \quad \& \quad \alpha + \alpha^\sigma + \alpha^{\sigma^2} \equiv 0 \pmod{p},$$

and their conjugates.

Thus the three regulators are zero modulo p . But for θ , \mathcal{L}^θ is generated by $U = e_\theta(1 - \tau)$ and by σU ; we have $\sigma^2 U = -U - \sigma U$, $\tau U = -U$, $\tau\sigma U = -\sigma^2 U$, $\tau\sigma^2 U = -\sigma U$ ($\mathcal{L}^\theta \simeq V_\theta$).

5.2.4. *Case $\eta = x^5 - 2x^4 + 4x^3 - 3x^2 + x - 1$, $p = 61$.* The G -module \mathcal{L} is generated by the three independent \mathbb{F}_p -linear relations (see [Gr4, Pr. A-13])

$$\begin{aligned} 19\alpha + 56\alpha^\sigma + 46\alpha^{\sigma^2} + \alpha^\tau &\equiv 0 \pmod{p} \\ 46\alpha + 19\alpha^\sigma + 56\alpha^{\sigma^2} + \alpha^{\tau\sigma^2} &\equiv 0 \pmod{p} \\ 56\alpha + 46\alpha^\sigma + 19\alpha^{\sigma^2} + \alpha^{\tau\sigma} &\equiv 0 \pmod{p}. \end{aligned}$$

The idempotent e_1 gives the trivial relation (because $19+56+46+1 \equiv 0 \pmod{61}$), thus the Fermat quotient of $\Delta_p^1(\eta)$ is nonzero modulo p .

We obtain the χ_1 -relation corresponding to the idempotent e_{χ_1} by summation of the three relations, which yields

$$\alpha + \alpha^\sigma + \alpha^{\sigma^2} - \alpha^\tau - \alpha^{\tau\sigma} - \alpha^{\tau\sigma^2} \equiv 0 \pmod{p}$$

(whence for $\theta = \chi_1$ the nullity modulo p of the θ -regulator $\Delta_p^\theta(\eta)$).

In fact it is a trivial nullity, the program finding that all the primes p are solution for $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$; the conjugates of η satisfy to

$$\eta^{1+\sigma+\sigma^2-\tau-\tau\sigma-\tau\sigma^2} = 1.$$

The choice of η being random, this fact was a pure coincidence !

For $\theta = \chi_2$ (of degree 2), the θ -regulator $\Delta_p^\theta(\eta)$ is zero modulo p (non trivially) and this corresponds to the following θ -relation by use of $e_\theta = \frac{1}{3}(2 - \sigma - \sigma^2)$

$$-\alpha + 36\alpha^\sigma + 26\alpha^{\sigma^2} + 21\alpha^\tau + 20\alpha^{\tau\sigma} + 20\alpha^{\tau\sigma^2} \equiv 0 \pmod{p}.$$

By conjugation, this last relation generates a \mathbb{F}_p -space of dimension 2 (in other words, $\mathcal{L}^\theta \simeq V_\theta$). Indeed, for the corresponding θ -relation

$$U = -1 + 36\sigma + 26\sigma^2 + 21\tau + 20\tau\sigma + 20\tau\sigma^2,$$

we have by definition $\sigma^2 U = -U - \sigma U$ and we find the relations $\tau U = 24U + 51\sigma U$, $\tau\sigma U = 27U + 37\sigma U$, $\tau\sigma^2 U = 10U + 34\sigma U$.

5.2.5. *Case* $\eta = 3x^5 - 20x^4 + 15x^3 + 16x^2 + 9x + 21$, $p = 7$. We find

$$\alpha \equiv \alpha^\sigma \equiv \alpha^{\sigma^2} \equiv 6x^5 + 2x^4 + 4x^3 + 3x^2 + 6 \pmod{p},$$

$$\alpha^\tau \equiv \alpha^{\tau\sigma} \equiv \alpha^{\tau\sigma^2} \equiv x^5 + 5x^4 + 3x^3 + 4x^2 + 6 \pmod{p}.$$

This case for which the G -module \mathcal{L}^θ is of \mathbb{F}_p -dimension 4 ($\mathcal{L}^\theta \simeq 2V_\theta \simeq e_\theta \mathbb{F}_p[G]$) is very rare, as we have seen § 4.4.3 (probability $\frac{O(1)}{p^4}$), because we must take η in such a way that $\text{rg}(F) = 6$ and that none of the $\Delta_p^\chi(\eta)$, $\chi = 1, \chi_1$, be zero modulo p , which is here the case.

6. SETS OF RESIDUES MODULO p IN Z_K

The application of the Borel–Cantelli principle only depends on the obstruction of minimal p -divisibility (Definition 4.1). So we propose in this section and the next one to remove this obstruction by means of the same heuristic used in [Gr2] for Fermat quotients of rational integers.

The fundamental point being the use of the Archimedean metric together with the p -adic one.

6.1. Definition of sets of residues.

6.1.1. *Recalls on Fermat quotients.* In the case $K = \mathbb{Q}$, we work in the set of residues $\mathcal{I}_p := [1, p[$ to find the $z \in \mathcal{I}_p$ such that $\Delta_p^1(z) = q_p(z) \equiv 0 \pmod{p}$ (cf. § 2.3.3 (i)) or more generally $\Delta_p^1(z) \equiv u \pmod{p}$ for a given $u \in [0, p[$. We then study the invariants $m_p(u)$ (number of $z \in \mathcal{I}_p$ such that $\Delta_p^1(z) \equiv u \pmod{p}$) and

$$M_p = \max_{u \in [0, p[} (m_p(u))$$

(maximal number of repetitions of the Fermat quotient). Then, we observe the stability of $M_p = O(\log(p))$, or $M_p = \frac{\log(p)}{\log_2(p)} \cdot (1 + \epsilon(p))$ (see [Gr5] for improvements and discussion about this question), then the fact that a $u_0 \in [0, p[$ such that $m_p(u_0) = M_p$ is random, and that the proportion of Fermat quotients obtained in $[0, p[$, by at least a $z \in \mathcal{I}_p$, tends to $1 - e^{-1} \approx 0.63212$ when $p \rightarrow \infty$.

It is the analysis of these numerical results which suggests the existence of a binomial law of probability on the $m_p(u)$, $u \in [0, p[$, with parameters $(p - 1, \frac{1}{p})$, giving :

$$\text{Prob}(m_p(u) \geq m) = \frac{1}{p^{p-1}} \sum_{j=m}^{p-1} \binom{p-1}{j} (p-1)^{p-1-j} \quad ([\text{Gr2, Section 4}]).$$

In particular, the probability to have $m_p(u) \geq 1$, (i.e., $u \in [0, p[$ is reached), is precisely rapidly equal to $1 - e^{-1} \approx 0.63212$ when $p \rightarrow \infty$.

If we apply this heuristic to $a \geq 2$ fixed and $\Delta_p^1(a) \equiv 0 \pmod{p}$, $p \rightarrow \infty$, the solutions $z \in \mathcal{I}_p$ to $\Delta_p^1(z) \equiv 0 \pmod{p}$ are at least $h := \lfloor \frac{\log(p)}{\log(a)} \rfloor$ in number (for the $z = a^j$, $1 \leq j \leq h$, and are said *exceptional solutions*), in which case, an elementary analytical calculation gives a probability of the form

$$\text{Prob}(q_p(a) \equiv 0 \pmod{p}) \leq \frac{O(1)}{p^{\log_2(p)/\log(a) - O(1)}}, \text{ for } p \rightarrow \infty.$$

As $M_p = O(\log(p))$ and since $M_p \geq m_p(0) \geq h$ in the case of such exceptional solutions, one can say that $M_p \approx m_p(0) \approx h = O(\log(p))$, even if $M_p > m_p(0)$ for some reasons explained § 7.2.6 (i).

When $m_p(0) = O(\log(p))$ (or $m_p(0) = M_p$) without the existence of $a \ll p$ such that $\Delta_p^1(a) \equiv 0 \pmod{p}$, we shall speak of *abundant solutions* for the $z \in \mathcal{I}_p$ such that $\Delta_p^1(z) \equiv 0 \pmod{p}$. This means that a number almost maximal of repetitions to $\Delta_p^1(z) \equiv u \pmod{p}$ takes place for $u = 0$. The case of exceptional solutions is a (rarest) particular case of abundant solutions.

6.1.2. *Generalization for dimension $n > 1$.* In the case of a field $K \neq \mathbb{Q}$, the ring of integers Z_K is of \mathbb{Z} -dimension $n > 1$, and similarly for Z_K/pZ_K as \mathbb{F}_p -vectoriel space. Consequently, a natural set \mathcal{I}_p in this case is for instance

$$\mathcal{I}_p = \left\{ \sum_{i=1}^n z_i e_i, \ z_i \in]-\frac{p}{2}, \frac{p}{2}[\ \forall i \right\},$$

where $(e_i)_{i=1, \dots, n}$ is a \mathbb{Z} -basis of Z_K . The other choice $z_i \in [1, p[$ is not possible because we need a complete set of residues modulo pZ_K being also “Archimedean”, that is to say of the form $\{z \in Z_K, |z|_\infty < R\}$, where R simply depends on p , as for $R = \frac{p}{2}$, because, contrary to the case $n = 1$, $e_1 = 1$, the signs are not controlled (especially if K is not real).

As for dimension 1, the fondamental principle still consists in the consideration of a fixed $\eta \in Z_K$ with primes $p \rightarrow \infty$, such that $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$, to remark that the first powers η^j of η are still in \mathcal{I}_p (Lemma 6.5) and verify $\Delta_p^\theta(\eta^j) \equiv 0 \pmod{p}$ (Theorem 6.6), giving $O(\log(p))$ exceptional solutions leading to the same conclusion as for the case $K = \mathbb{Q}$.

On the other hand, for $n > 1$, the probabilistic study of the $\Delta_p^\theta(z)$, $z \in \mathcal{I}_p$ (in particular the computation of the $m_p(u)$ and of M_p), is numerically out of range for very large prime numbers p (program with loops needing p^n calculations) and we must define another process allowing the use of large p , while preserving the statistical relevance.

Before we can give an overview of these computations in \mathcal{I}_p for dimension $n > 1$ by means of the cyclic cubic field $K = \mathbb{Q}(x)$, $x = \zeta_7 + \zeta_7^{-1}$, where ζ_7 is a 7th root of unity (Pr. B of [Gr4]). Put

$$z = ax^2 + bx + c \in \mathcal{I}_p, \quad a, b, c \in]-\frac{p}{2}, \frac{p}{2}[.$$

To limit ourselves to the conditions of Definition 4.1, we suppose $p \equiv 1 \pmod{3}$ and we fixe $\theta \neq 1$ (defined by means of $r \in [1, p[$ of order 3 modulo p).

This raises the problem of weighting the values $m_p(u)$ and M_p (very large); we have computed the quantities $m'_p(0) = \frac{m_p(0)}{N_p}$, $M'_p = \frac{n(p-1)M_p}{N_p}$, where $N_p = p^3 - 1$ or $(p-1)^3$ (depending on whether $n_p = 3$ or 1) is the number of triples (a, b, c) such that z is prime to p ; these quantities coincide with the expressions of the case $n = 1$. We denote by u an element of $[0, p[$ which realises M_p .

The case of M'_p is more difficult concerning a possible multiplicative constant (the factor n seems coherent since it takes into account the action of G on \mathcal{I}_p when this set is a G -module, case where the chosen basis is a normal basis). We still obtain $M'_p = O(\log(p))$.

For primes $p < 67$, the value of $\frac{M'_p}{\log(p)} = \frac{3(p-1)M_p}{N_p \times \log(p)}$ is near from 1, but it seems that this quantity is decreasing and rapidly bounded by 1; the case $p = 61$ is

particular because $u = 0$ (exceptional solutions: $m'_p = 1.92651$, $\frac{M'_p}{\log(p)} = 1.41159$)

$p = 67$	$n_p = 3$	$u = 9$	$N_p = 300762$
$m'_p(0) = 0.98046$	$M_p = 4732$	$M'_p = 3.11520$	$\frac{3(p-1)M_p}{N_p \times \log(p)} = 0.74354$
$p = 73$	$n_p = 3$	$u = 5$	$N_p = 389016$
$m'_p(0) = 0.99537$	$M_p = 5568$	$M'_p = 3.09161$	$\frac{3(p-1)M_p}{N_p \times \log(p)} = 0.72290$
\dots			
$p = 139$	$n_p = 1$	$u = 72$	$N_p = 2628072$
$m'_p(0) = 0.99107$	$M_p = 19322$	$M'_p = 3.04379$	$\frac{3(p-1)M_p}{N_p \times \log(p)} = 0.61684$
$p = 151$	$n_p = 3$	$u = 75$	$N_p = 3442950$
$m'_p(0) = 0.97416$	$M_p = 23458$	$M'_p = 3.06600$	$\frac{3(p-1)M_p}{N_p \times \log(p)} = 0.61108$

6.1.3. *Another approach for dimension $n > 1$.* The problem is multiplicative since the $O(\log(p))$ first powers of η must belong to the Archimedean set $I_p \subseteq \mathcal{I}_p$ (I_p to be defined) which must contain the exceptionnal solutions when $\Delta_p^g(\eta) \equiv 0 \pmod{p}$. Moreover, the numerical aspect needs to work in a “structure of dimension 1” by analogy with the case $K = \mathbb{Q}$. Give for this the following definitions:

Definition 6.1. We make choice of an integer basis $(e_i)_{i=1,\dots,n}$ of K , and for all

$\gamma \in Z_K$ we put $\gamma = \sum_{i=1}^n c_i e_i$, $c_i \in \mathbb{Z}$ for all i .

(i) We call residue modulo p of γ the integer $[\gamma]_p := \sum_{i=1}^n [c_i]_p e_i$ of Z_K , with

$$[c_i]_p \in]-\frac{p}{2}, \frac{p}{2}] \text{ \& } c_i \equiv [c_i]_p \pmod{p}.$$

(ii) We define the set of residues $I_p(\gamma) := \{[\gamma^k]_p, k \in [1, p[\}$.

(iii) We denote by $z = \sum_{i=1}^n z_i e_i$, $z_i \in]-\frac{p}{2}, \frac{p}{2}]$ for all i , any element of $I_p(\gamma)$.

In the case $n = 1$ of the Fermat quotient of fixed $\eta = a$, if $\gamma = g$ is a primitive root modulo $p > 2$, $I_p(g) := \{[g^k]_p, k \in [1, p[\} = \{-\frac{p-1}{2}, \dots, -1, 1, \dots, \frac{p-1}{2}\}$ (up to the order). The set $\{[a^k]_p, k \in [1, p[\} \subseteq I_p(g)$ has a periodicity if a is not a primitive root modulo p and we must not base the statistical study on this set, but on $I_p(g)$. Moreover, the group of roots of unity (here ± 1) must be taken into account.

In the general case, let μ_K be the group of roots of unity of the field K . We denote by D the order of η in $(Z_K/pZ_K)^\times \simeq \prod_{v|p} F_v^\times$, $F_v \simeq \mathbb{F}_{p^{n_p}}$, and by $d|D$ the

order of η in $\left(\prod_{v|p} F_v^\times\right) / i_p(\mu_K)$, where we suppose that η generates a multiplicative $\mathbb{Z}[G]$ -module of rank n . We have the following result for all prime p large enough:

Lemma 6.2. (i) *There exists $\gamma \in Z_K$ such that $[\eta]_p = [\gamma^{(p^{n_p}-1)/D}]_p$.*

(ii) *If $n_p > 1$, then d (hence D) does not divide $p-1$.*

(iii) *We have $D \geq d \geq \frac{\log(p-1)}{\log(c_0(\eta))}$, where $c_0(\eta) = \max_{\sigma \in G}(|\eta^\sigma|)$.*

Proof. (i) For all $v|p$, let $g_v \in Z_K$ whose image in F_v^\times is a generator, and let η_v be the image of η . We put $\eta_v = g_v^{\lambda_v}$ then $\eta_v = g_v^{\lambda \mu_v}$ where $\lambda = \text{p.g.c.d.}((\lambda_v)_v)$. Then $(g_v^{\mu_v})_v$ is of order $p^{n_p} - 1$. It is sufficient to take $\gamma \in Z_K$ whose diagonal image in $\prod_{v|p} F_v^\times$ is equal to $(g_v^{\mu_v})_v$ to obtain $\eta \equiv \gamma^\lambda \pmod{p}$.

Replacing γ by γ^μ , μ prime to $p^{n_p} - 1$, one may suppose that $\lambda = \frac{p^{n_p}-1}{D}$.

(ii) Let $v|p$ and let $\tau_v \in G$ be the corresponding Frobenius automorphism; it is such that $\eta^{\tau_v} \equiv \eta^p \pmod{\mathfrak{p}_v}$ in K , whence $\eta^{\tau_v-1} \equiv \eta^{p-1} \pmod{\mathfrak{p}_v}$. If we suppose $\eta^{p-1} \equiv \zeta \pmod{p}$, $\zeta \in \mu_K$ of order $r \geq 1$, then $\eta^{r(\tau_v-1)} \equiv 1 \pmod{\mathfrak{p}_v}$, which leads to $\eta^{r\tau_v} \equiv \eta^r \pmod{\mathfrak{p}_v}$. But the integer $\eta^{r\tau_v} - \eta^r$ is nonzero since η^r is not in a strict subfield of K and if $\mathcal{D}(\eta^r)$ is its discriminant, it is a nonzero rational integer hence not divisible by p for all p large enough (absurd).

(iii) We have $\eta^d = \zeta + \Lambda p$, where $\zeta \in \mu_K$, $\Lambda \in Z_K \setminus \{0\}$. Up to conjugation, one may suppose that $|\Lambda| \geq 1$. This yields $|\eta|^d \geq |\Lambda|p - |\zeta| \geq p - 1$, and finally $d \geq \frac{\log(p-1)}{\log(|\eta|)} \geq \frac{\log(p-1)}{\log(c_0(\eta))}$. \square

The set $\{[\gamma^t]_p, t \in [0, p^{n_p}]\}$ is the union of p^{n_p-1} sets $I_p^{(\lambda)} = \{[\gamma^{\lambda p+k}]_p, k \in [0, p]\}$, $\lambda \in [0, p^{n_p-1}]$. A first heuristic is to say that these sets $I_p^{(\lambda)}$ have the same statistical behavior concerning the numbers $m_p(u)$ and M_p . We may in general consider the set $I_p(\gamma) := \{[\gamma^k]_p, k \in [1, p]\}$. We distinguish two cases about numerical experiment:

a) Case $n_p > 1$. In general $|I_p(\eta)| = p - 1$ except if $D < p$ (e.g. $p = 5$, $n_p = 2$, $\eta^3 \equiv 1 \pmod{p}$). But when $p \rightarrow \infty$ one can use the following heuristic/conjecture:

Heuristic 6.3. *We suppose that K is distinct from \mathbb{Q} and from a quadratic field. The primes p for which $n_p > 1$ and η is of order D modulo p , with $D < p$, are finite in number.*

Put $n = n_p g_p$ and let $(\eta_v)_v|_p$ be the image of η in $\prod_{v|p} F_v^\times$. To say that η is of order a divisor of D modulo p is equivalent to the g_p independent conditions $\eta_v^D = 1$ for all $v|p$ whose probability is $\left(\frac{D}{p^{n_p}-1}\right)^{g_p} \sim \frac{D^{g_p}}{p^{n_p g_p}}$. If we sum over the $D < p$, we obtain the upper bound $O(1) \frac{p^{g_p+1}}{p^{n_p g_p}} = \frac{O(1)}{p^{n_p g_p - g_p - 1}}$, which is clear for $(n_p - 1)g_p > 2$ and needs a particular study in the case $n_p = 1$ and in the case of a quadratic field K with p inert.

In this last case, we can define a “structure of dimension 1” in the following way. We replace η by $\eta' = \eta^{\tau-1}$ where τ , is a generator of G and the Frobenius automorphism at p ; we then have $\eta' \equiv \eta^{p-1} \pmod{p}$ and η' is of order $D'|p+1$ modulo p . There exists γ of order $p+1$ modulo p such that $I_p(\gamma)$ contains $\eta' \equiv \gamma^{(p+1)/D'} \pmod{p}$. As $\eta^{2\tau} = \eta^{\tau+1}\eta' =: a\eta'$ the theory of the $\Delta_p^\theta(\eta)$ is identical to that of $\Delta_p^\theta(\eta')$ for $\theta \neq 1$ and moreover, η' is independent of p and remains “small”. We shall have $[\eta'^j]_p = \eta'^j$ for $1 \leq j \leq h' = O(h)$ because $D' > h'$ as in Lemma 6.2.

Remark 6.4. By using an analytical argument of [T], one may replace $\frac{O(1)}{p^{n_p g_p - g_p - 1}}$

by the upper bound $\frac{C_\epsilon}{p^{n_p g_p - g_p - \epsilon}}$ (for all $\epsilon > 0$ and p large enough), which allows us to eliminate cubic and quartic cases, but not the quadratic case for which we have conjecturally infinitely many solutions p (cf. [Gr6]).

The point (ii) of Lemma 6.2 enforces this heuristic. Thus we shall base the statistical study on $I_p = I_p(\eta)$. We admit, as for the case of Fermat quotients (cf. [H-B]), that the $\Delta_p^\theta(z)$ are uniformly distributed from any set with $p - 1$ elements of residues z generated by the powers of a fixed integer.

b) Case $n_p = 1$ (p totally split in K). The order D of η modulo p is a divisor of $p-1$ and the probability for this order to be a strict divisor of $p-1$ is $1 - \frac{\phi(p-1)}{p-1}$, where ϕ is the Euler function, which roughly is between $\frac{1}{2}$ and $1 - \frac{1.781}{\log_2(p)}$. So we cannot consider $I_p(\eta)$. We use Lemma 6.2 (i) to create a set of residues of the form $I_p(\gamma) = \{[\gamma^k]_p, k \in [1, p[\}$ which contains $[\eta]_p$ and which has $p-1$ elements. We may always choose γ such that $[\eta]_p = [\gamma^{(p-1)/D}]_p$.

From Lemma 6.2 (iii), $I_p(\gamma)$ contains $d = O(\log(p))$ distinct residues of the form $[\eta^j]_p$ for $1 \leq j \leq d$ which are not in μ_K .

For the numerical experiments, we shall use $I_p = I_p(\gamma)$ generated by a γ having the good generating properties because the goal is to verify the validity of the existence of a binomial probability law for the values of the $m_p(u)$, which is a property of I_p and not a property of its elements; in other words, I_p must be the analogue of $I_p(g)$ for the dimension 1 and if we study a fixed η (analogue of $a \geq 2$ for the dimension 1) when $p \rightarrow \infty$, one may say that η belongs to a suitable $I_p(\gamma)$ in which the heuristic applies (as for $a \in I_p(g)$).

The programs do not make the distinction between η and γ insofar as the case $|I_p| < p-1$ is very rare. We suppress from I_p the roots of unity $\zeta \in \mu_K$ because $\alpha_p(\zeta) = 0$ would modify the statistics (we still meet this case in dimension 1 where $\{-1, 1\} \subset I_p =] - \frac{p-1}{2}, \frac{p-1}{2} [$).

After, for the computation of the $m_p(u)$ and of M_p , relative to I_p , we shall prove that if $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$ (analogue of $q_p(a) \equiv 0 \pmod{p}$), we have $\Delta_p^\theta(\eta^j) \equiv 0 \pmod{p}$ (analogue of $q_p(a^j) \equiv 0 \pmod{p}$), for all $j \leq h = O(\log(p))$ (Lemma 6.5 and Theorem 6.6 below).

6.1.4. Fundamental Archimedean principle. If for instance, $\eta = \gamma = 2 + i \in \mathbb{Z}[i]$, with $i^2 = -1$, this yields $\eta^2 = 3 + 4i$, $\eta^3 = 2 + 11i$, $\eta^4 = -7 + 24i$, $\eta^5 = -38 + 41i$, $\eta^6 = -117 + 44i$, $\eta^7 = -278 - 29i, \dots$

We see that if $p \rightarrow \infty$, the residues $[\eta^j]_p$ will coincide with the exact values (not reduced), η^j , for a finite number of indices j , and after we shall have the corresponding residues; for $p = 47$ we get $] - \frac{p}{2}, \frac{p}{2} [= [-23, 23]$ and

$$I_p = \{[\eta]_p = \eta, [\eta^2]_p = \eta^2, [\eta^3]_p = \eta^3, [\eta^4]_p = -7 - 23i, [\eta^5]_p = 9 - 6i, [\eta^6]_p = -23 - 3i, [\eta^7]_p = 4 + 18i, \dots\}.$$

More precisely, we have the following result:

Lemma 6.5. *Let $\eta \in Z_K \setminus \{0\}$, be an integer of K , distinct from a root of unity, and let $c_0(\eta) = \max_{\sigma \in G} (|\eta^\sigma|)$. Then there exists an explicit constant $\Gamma(K) \geq 1$, independent of η and p , such that $[\eta^j]_p = \eta^j$ for all j such that*

$$1 \leq j \leq \frac{\log(p-1) - \log(2\Gamma(K))}{\log(c_0(\eta))}$$

(since $|N_{K/\mathbb{Q}}(\eta)| \geq 1$ and η is not a root of unity, we have $c_0(\eta) > 1$).

Proof. Put $\eta^j = \sum_{i=1}^n A_{j,i} e_i$, $A_{j,i} \in \mathbb{Z}$ for all $i = 1, \dots, n$. We have $\eta^{j\sigma} = \sum_{i=1}^n A_{j,i} e_i^\sigma$ for all $\sigma \in G$. The matrix $(e_i^\sigma)_{i,\sigma}$ is invertible (the square of its determinant is the discriminant of the field K); the coefficients Γ_i^σ of the inverse matrix are elements of K independent of η, p, j , and

$$A_{j,i} = \sum_{\sigma \in G} \Gamma_i^\sigma \eta^{j\sigma}, \quad i = 1, \dots, n.$$

A sufficient condition to have $|A_{j,i}| < \frac{1}{2}p$ for all i , is that a common upper bound of these numbers be less than $\frac{1}{2}(p-1)$. But we have

$$\left| \sum_{\sigma \in G} \Gamma_i^\sigma \eta^{j\sigma} \right| \leq \sum_{\sigma \in G} |\Gamma_i^\sigma| |\eta^{j\sigma}| \leq c_0(\eta)^j \sum_{\sigma \in G} |\Gamma_i^\sigma|.$$

Put

$$(6.1) \quad \Gamma(K) := \max_{i=1, \dots, n} \left(\sum_{\sigma \in G} |\Gamma_i^\sigma| \right)$$

(maximum of the sums of the lines); then it is sufficient to have

$$c_0(\eta)^j \cdot \Gamma(K) \leq \frac{1}{2}(p-1),$$

whence the result. If $1 = \sum_{k=1}^n \lambda_k e_k$, $\lambda_k \in \mathbb{Z}$, we have

$$\sum_{\sigma \in G} \Gamma_i^\sigma \times 1^\sigma = \sum_{\sigma \in G} \sum_{k=1}^n \Gamma_i^\sigma \lambda_k e_k^\sigma = \sum_{k=1}^n \delta_{i,k} \lambda_k = \lambda_i, \text{ for all } i;$$

there exists at least an index i such that $\sum_{\sigma \in G} |\Gamma_i^\sigma| \geq 1$. \square

The general case is thus analogous to that of Fermat quotients and leads to the following result with the notation of Lemma 6.5:

Theorem 6.6. *Let $\eta \in Z_K$ generating a multiplicative $\mathbb{Z}[G]$ -module of rank n . Let p be large enough and let $I_p = I_p(\gamma)$ (Definition 6.1) be such that $|I_p| = p-1$ and such that $\eta \in I_p$; let θ be an irreducible p -adic character of G .*

If $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$ we have $z_j := \eta^j \in I_p$ and $\Delta_p^\theta(z_j) \equiv 0 \pmod{p}$ for all j such that $1 \leq j \leq h$, where $h = h_p(\eta) := \frac{\log(p-1) - \log(2\Gamma(K))}{\log(c_0(\eta))}$ (Lemma 6.5 and Relation (6.1)). Moreover, $z_j \notin \mu_K$.

Proof. Put $\eta = [\gamma^e]_p$. The case $n_p > 1$ where $\gamma = \eta$ is obvious since $e = 1$. If $n_p = 1$ and $\eta = \gamma^{\frac{p-1}{D}}$, $e = (p-1)/D$ and Lemma 6.2 (iii) shows that

$$D \geq d \geq \frac{\log(p-1)}{\log(c_0(\eta))} > h;$$

consequently, the conditions $eh \leq p-1$ and $z_j \notin \mu_K$ are always fulfilled. We know that $\alpha_p(\eta^j) \equiv j\alpha_p(\eta) \pmod{p}$ for all j and that we have $\eta \equiv \gamma^e \pmod{p}$, $e \in [1, p[$. If we restrict ourselves to the $j \leq h$, we get $\eta^j \equiv \gamma^{ej} \pmod{p}$ and $\eta^j = [\eta^j]_p = [\gamma^{ej}]_p =: z_j \in I_p$ since $ej \leq p-1$.

By definition of the G -modules \mathcal{L}^θ (whose non triviality is equivalent to the nullity of the corresponding Δ_p^θ), we have $\mathcal{L}^\theta(\eta^j) = \mathcal{L}^\theta(\eta)$ in $\mathbb{F}_p[G]$ because any θ -relation $\sum_{\nu \in G} u(\nu) \alpha_p(\eta)^\nu \equiv 0 \pmod{p}$, coming from $\mathcal{L}^\theta(\eta)$, is equivalent to

$$\sum_{\nu \in G} u(\nu) \alpha_p(\eta^j)^\nu \equiv j \cdot \sum_{\nu \in G} u(\nu) \alpha_p(\eta)^\nu \equiv 0 \pmod{p},$$

$j \leq h$ never being divisible by p . So the $\Delta_p^\theta(\eta^j)$, characterized via the $\mathcal{L}^\theta(\eta^j)$, are all zero modulo p as soon as $\Delta_p^\theta(\eta)$ is zero, and as was said, $\eta^j \in I_p$ for $1 \leq j \leq h$. This implies the existence of at least $h = O(\log(p))$ exceptional solutions, relatively to the integer η . \square

7. REMOVAL OF THE OBSTRUCTION OF MINIMAL p -DIVISIBILITY

7.1. The invariants $m_p(u)$ and M_p . For given p , θ and $u \in [0, p[$, let $m_p(u)$ be the number of $z \in I_p$ having a θ -regulator $\Delta_p^\theta(z)$ congruent to u modulo p . We denote by

$$M_p = \max_{u \in [0, p[} (m_p(u))$$

the *maximal number of repetitions*. We suppose a part of the conditions of Definition 4.1 for p and θ , namely $f = \delta = 1$.

We then obtain a remarkable stability for M_p , very regular function of p which can be the subject of the following heuristic as for Fermat quotients (§6.1.1):

Heuristic 7.1. *For all $p \geq 2$ and all irreducible p -adic character θ of G , given such that $f = \delta = 1$ (cf. Definition 4.1), the number $M_p = \max_{u \in [0, p[} (m_p(u))$ of residues $z \in I_p$ having, modulo p , the same local θ -regulator, is $O(\log(p))$ (see [Gr5] for more discussion about this).*

As the mean value of $m_p(0)$ is near from 1, the abundant case (i.e., when $m_p(0) = O(\log(p))$) is as rare as the exceptional case (i.e., when $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$), generating $h = O(\log(p))$ solutions in I_p of the form η^j , $j = 1, \dots, h$.

7.2. Numerical experiments. Let us give numerical justifications for properties of $m_p(u)$ and M_p . In the programs and results hereinafter, we start from a very simple numerical value of γ (many experiments have shown a high stability of results regarding this choice) and we compute the set I_p of residues z of the form $[\gamma^k]_p$, $k = 1, \dots, p-1$, then the values $\Delta_p^\theta(z) \pmod{p}$ which are managed in a list L to determine $m_p(0)$ and $M_p = m_p(u_0)$ for a suitable u_0 .

We shall take $\gamma = \eta$ if I_p satisfies the conditions mentioned §6.1.3.

7.2.1. Cyclic cubic case, p inert in $\mathbb{Q}(j)$ ($j^3 = 1$, $j \neq 1$), $\theta \neq 1$. In this case, the statistical study of the $\Delta_p^\theta(z)$, for $z \in I_p$, is not necessary as we have explained since from the main heuristic 4.2.2, we would have $\text{Prob}(\Delta_p^\theta(z) \equiv 0 \pmod{p}) = \frac{O(1)}{p^2}$; however, one can calculate the values $m_p(0)$ and M_p to see that $m_p(0) > 0$ is very rare and in order to see what happens for M_p .

Here, for $x = \zeta_7 + \zeta_7^{-1}$, let $K = \mathbb{Q}(x)$ be the cubic cyclic field of conductor 7, let $G = \{1, \sigma, \sigma^2\}$, and take $p \equiv -1 \pmod{6}$ (in other words $f = 2$).

For $\theta \neq 1$, we have

$$\Delta_p^\theta(z) = \alpha^2 + \alpha^{2\sigma} + \alpha^{2\sigma^2} - \alpha\alpha^\sigma - \alpha^\sigma\alpha^{\sigma^2} - \alpha^{\sigma^2}\alpha$$

(where $\alpha = \alpha_p(z)$), which is rational modulo p (Pr. B-1 of [Gr4]).

Let I_p be generated by $\gamma = x^2 + 2$; concerning the 328 prime numbers $p \equiv -1 \pmod{6}$, $5999 < p < 11999$, we have $m_p(0) > 0$ only for 5 values of p (i.e., $p = 6761, 7937, 8861, 9941, 10739$) and then 323 cases where $m_p(0) = 0$. But all the cases $m_p(0) > 0$ are due to the fact that there exists $d \mid p-1$, $d \neq p-1$, such that $\gamma^d \equiv \rho \pmod{p}$, where ρ is a rational; so, for $z = [\rho^d]_p$, $\Delta_p^\theta(z)$ is trivially zero modulo p , and these cases are to be excluded as explained §6.1.3.

For $p \equiv 1 \pmod{6}$, $6001 < p < 12001$, we shall find 134 values of p , among 327, for which $m_p(0) = 0$, and the numbers $m_p(0) \neq 0$ will have higher mean values. On the other hand, M_p does not seem to depend on the decomposition of p in $\mathbb{Q}(j)$.

We have extracted the following examples for $p \equiv -1 \pmod{6}$; the parameter $u_0 \in [0, p[$ furnishes an integer (among several a priori) such that $M_p = m_p(u_0)$

$p = 59999$	$n_p = 3$	$u_0 = 25910$
$m_p(0) = 0$	$M_p = 7$	$M_p/\log(p) = 0.63624$
$p = 60017$	$n_p = 1$	$u_0 = 51505$
$m_p(0) = 0$	$M_p = 7$	$M_p/\log(p) = 0.63622$
$p = 60029$	$n_p = 3$	$u_0 = 19677$
$m_p(0) = 0$	$M_p = 7$	$M_p/\log(p) = 0.63621$
$p = 60041$	$n_p = 3$	$u_0 = 59841$
$m_p(0) = 0$	$M_p = 8$	$M_p/\log(p) = 0.72708$

We have for instance $m_p(0) = 0$ and $M_p = 8$ for $p = 60041$ ($u_0 = 59841$), and we obtain the following residues $z = [\gamma^j]_p$ solutions to $\Delta_p^\theta(z) \equiv 59841 \pmod{p}$

exponent j	residues $[\gamma^k]_p$
12869	$-17167x^2 + 1730x + 28097$
31327	$17781x^2 + 4775x + 25387$
32191	$3615x^2 - 27037x - 25973$
39129	$6079x^2 + 24215x + 18753$
44870	$-11178x^2 + 24638x + 12843$
54374	$3053x^2 - 24995x - 12010$
56394	$-3461x^2 + 16186x + 7608$
56651	$-19244x^2 - 9845x + 3277$

7.2.2. *Cyclic cubic case, p splitted in $\mathbb{Q}(j)$ ($j^3 = 1, j \neq 1$).* We then have $p \equiv 1 \pmod{6}$, i.e., $f = 1$. There are two p -adic θ -regulators

$$\Delta_p^\theta(z) = \alpha + r^2 \alpha^\sigma + r \alpha^{\sigma^2},$$

where $\alpha = \alpha_p(z)$ and where r is one of the two elements of order 3 modulo p .

In that case, $\Delta_p^\theta(z)$ is a “resolvent of Hilbert modulo p ” which is congruent to a rational modulo the prime ideal \mathfrak{p} associated with θ . But Pr. B-2 of [Gr4] gives $\Delta_p^\theta(z) = u_2 x^2 + u_1 x + u_0$ which supposes that we use a congruence of the form $x \equiv R \pmod{\mathfrak{p}}$ in order to obtain $\Delta_p^\theta(z) \equiv u \pmod{p}$. We proceed in a different way: to get a rational, we multiply $\Delta_p^\theta(z)$ by

$$H := x + rx^\sigma + r^2 x^{\sigma^2} \pmod{p}$$

which serves as a “conjugate resolvent” once for all; it is not divisible by p .

We generate I_p by means of $\gamma = x^2 + 2$. We have extract the following examples

$p = 60037$	$n_p = 3$	$u = 26443$
$m_p(0) = 0$	$M_p = 8$	$M_p/\log(p) = 0.72709$
$p = 60091$	$n_p = 3$	$u = 32679$
$m_p(0) = 1$	$M_p = 7$	$M_p/\log(p) = 0.63615$
$p = 60103$	$n_p = 1$	$u = 22560$
$m_p(0) = 0$	$M_p = 9$	$M_p/\log(p) = 0.81789$
$p = 60127$	$n_p = 3$	$u = 55712$
$m_p(0) = 1$	$M_p = 7$	$M_p/\log(p) = 0.63612$

7.2.3. *Example of $M_p = m_p(u)$ for $u > 0$.* Still in $K = \mathbb{Q}(x)$, with $x = \zeta_7 + \zeta_7^{-1}$, we consider $\gamma = -5x^2 + 2x + 3$ (Pr. B-3 of [Gr4]). For $p = 5011$, we find a maximal

number $M_p = 7$ of $z \in I_p$ such that $\Delta_p^\theta(z) \equiv u_0 \pmod{p}$ for $u_0 = 418$ (we then have $m_p(0) = 1$ and $M_p/\log(p) = 0.82165$)

exponent j	residues $[\gamma^j]_p$
1233	$2043x^2 - 540x - 359$
1297	$810x^2 + 74x + 1078$
1932	$-1415x^2 + 962x - 1352$
2465	$577x^2 + 1380x + 1727$
2941	$-1735x^2 - 172x + 1553$
3848	$1168x^2 - 816x + 70$
4339	$-320x^2 - 426x + 468$

7.2.4. *Diedral case of order 6.* We consider the field $K = \mathbb{Q}(j, \sqrt[3]{2})$ (where j denotes a cubic root of unity), with Galois group $G = D_6 = \{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$, and the unique irreducible p -adic character θ of degree 2 for which (with $\alpha := \alpha_p(z)$)

$$\Delta_p^\theta(z) = \frac{1}{\sqrt{-3}}(\alpha^2 + \alpha^{2\sigma} + \alpha^{2\sigma^2} - \alpha^{2\tau} - \alpha^{2\tau\sigma} - \alpha^{2\tau\sigma^2} - \alpha\alpha^\sigma - \alpha^\sigma\alpha^{\sigma^2} - \alpha^{\sigma^2}\alpha + \alpha^\tau\alpha^{\tau\sigma} + \alpha^{\tau\sigma}\alpha^{\tau\sigma^2} + \alpha^{\tau\sigma^2}\alpha^\tau).$$

We use here I_p generated by $\gamma = 2x^5 + 2x^3 + x - 1$ (Pr. B-4 of [Gr4])

$p = 3559$	$u_0 = 2946$	
$m_p(0) = 1$	$M_p = 6$	$M_p/\log(p) = 0.73374$
$p = 3571$	$u_0 = 2286$	
$m_p(0) = 1$	$M_p = 5$	$M_p/\log(p) = 0.61120$
$p = 3581$	$u_0 = 1$	
$m_p(0) = 0$	$M_p = 7$	$M_p/\log(p) = 0.85539$
$p = 3583$	$u_0 = 1852$	
$m_p(0) = 0$	$M_p = 6$	$M_p/\log(p) = 0.73314$

We consider $\gamma = x^5 + 2x^4 - 2x^3 - x + 1$. For $p = 1709$, we obtain $m_p(0) = 1$ and $M_p = 6$ for $u_0 = 487$ (we have $M_p/\log(p) = 0.80605$); whence the array of the $z = [\gamma^j]_p$ such that $\Delta_p^\theta(z) \equiv 487 \pmod{p}$

exponent j	residues $[\gamma^j]_p$
51	$-179x^5 + 718x^4 + 739x^3 + 688x^2 + 553x - 159$
81	$-212x^5 - 730x^4 - 634x^3 + 849x^2 - 161x - 556$
759	$-649x^5 + 324x^4 - 729x^3 + 675x^2 - 423x + 149$
1079	$552x^5 - 364x^4 + 136x^3 + 52x^2 + 799x + 335$
1291	$651x^5 + 584x^4 + 334x^3 + 263x^2 + 437x + 624$
1567	$99x^5 + 566x^4 - 292x^3 + 152x^2 + 529x - 645$

We shall examine in which way it is possible to have $m_p(0) = O(\log(p))$ (abundant solutions) apart from the case of exceptional solutions, important point to justify the existence of a binomial probability law.

7.2.5. *Cas where $m_p(0) = O(\log(p))$ apart from the exceptional case.* We intend to give numerical examples of prime numbers p for which I_p (generated by $\gamma = \eta \ll p$) has $m_p(0) = O(\log(p))$ solutions $z \in I_p$ to $\Delta_p^\theta(z) \equiv 0 \pmod{p}$, in the case where these solutions are not of the form

$$\mu^j = [\mu^j]_p, 1 \leq j \leq h' = \left\lfloor \frac{\log(p-1) - \log(2\Gamma(K))}{\log(c_0(\mu))} \right\rfloor$$

of the exceptional case when $\Delta_p^\theta(\mu) \equiv 0 \pmod{p}$, $\mu \ll p$. The numerical experiments show that this is as rare as in the exceptional case and we shall conclude on these various cases in § 7.2.6.

(i) Case $G = 1$. Although this has been studied in [Gr2] (array of § 4.3.1 giving pairs $(p, m_p(0))$ with $m_p(0) \geq 6$), by comparison one may see again the case of Fermat quotient for which we always have $I_p = [1, p[$.

We obtain the following array in which we have fixed $a = 14$, to find cases $q_p(a) \equiv 0 \pmod{p}$ (exceptional solutions a^j) and the cases $m_p(0) = O(\log(p))$ (abundant solutions z), for primes p such that $3 \leq p \leq 10007$ (Pr. B-0 of [Gr4])

p	$u \in [0, p[$ tels que $q_p(z) = u$ for $M_p = m_p(u)$	M_p	$m_p(0)$
$p = 11$	<i>abundant</i> ($z = 3, 9$) $u = 0, 5$	$M_p = 2$	$m_p(0) = 2$
$p = 29$	<i>exceptional</i> ($z = 14$) $u = 24, 16, 1$	$M_p = 3$	$m_p(0) = 1$
$p = 353$	<i>exceptional</i> ($z = 14, 196$) $u = 297, 275$	$M_p = 6$	$m_p(0) = 2$
$p = 653$	<i>abundant</i> ($z = 84, 120, 197, 287, 410$) $u = 0, 99, 360, 241, 353, 617, 119, 399$	$M_p = 5$	$m_p(0) = 5$
$p = 4909$	<i>abundant</i> ($z = 2189, 2234, 2406, 3266, 4649$) $u = 0, 4651, 2785, 3967, 648, 3544, 3322, 2381, 1843, 3465, 1089, 1483, 4171$	$M_p = 5$	$m_p(0) = 5$
$p = 5107$	<i>abundant</i> ($560, 1209, 1779, 2621, 4295, 4361$) $u = 0, 2705, 4159$	$M_p = 6$	$m_p(0) = 6$

(ii) Case $G = C_3$ (Pr. B-5 of [Gr4]). We use the cubic cyclic field of conductor 7 and I_p generated by $\gamma = x^2 + x + 2$.

For $p = 2053$ (the least example with $M_p = m_p(0) = 7$) we obtain the following residues $z = [\gamma^j]_p$ such that $\Delta_p^\theta(z) \equiv 0 \pmod{p}$ (for the unique $u_0 = 0$)

exponent j	residues $[\gamma^j]_p$
186	$871x^2 - 930x + 496$
500	$57x^2 + 272x + 478$
559	$-691x^2 - 1003x - 881$
1399	$258x^2 + 1002x - 349$
1870	$-375x^2 - 212x + 240$
1981	$-464x^2 + 818x - 783$
2034	$121x^2 + 610x + 524$

The example is clear since the exponents j are not the first powers of a $\mu \in I_p$, $\mu \ll p$, and since there are no other solutions.

For I_p generated by $\gamma = 2x^2 + x + 3$ and $p = 1987$, we have $M_p = m_p(0) = 5$ for $u = 1026, 454, 282, 180, 0, 1734, 117, 325, 1225$ and an analogous array of residues for $u_0 = 0$.

For $\gamma = 2x^2 + x + 2$, $p = 37, 307, 2347$ give non exceptional abundant solutions. Only $p = 79$ leads to a mixed case ($M_p = m_p(0) = 4$), with $u = 0, 71$ and the array of residues for $u_0 = 0$

exponent j	residues $[\gamma^j]_p$
1	$2x^2 + x + 2$
2	$17x^2 + 8x + 4$
20	$19x^2 - 11x + 15$
35	$-35x^2 - 33x + 19$

(iii) Dihedral case of degree 6 (Pr. B-6 of [Gr4]). The character θ of degree 2 allows us to confirm the previous computations. For abundant solutions, the $m_p(0) \approx M_p$ maximum, equal to 6, is given by the following example, where I_p , for $p = 331$, is

generated by the integer $\gamma = -x^5 + x^4 - x^3 - x^2 + 1$

exponent j	residues $[\gamma^j]_p$
48	$59x^5 - 46x^4 - 87x^3 + 141x^2 + 158x + 40$
102	$-61x^5 - 114x^4 + 119x^3 + 11x^2 - 125x - 120$
138	$-123x^5 - 122x^4 - 79x^3 - 61x^2 + 22x - 71$
155	$91x^5 + 100x^4 + 136x^3 + 138x^2 + 152x + 147$
180	$152x^5 - 8x^4 - 59x^3 - 165x^2 + 92x - 131$
322	$49x^5 - 158x^4 - 13x^3 - 14x^2 - 33x - 23$

For $\gamma = -x^5 - x^4 + x^3 - x^2 - x + 1$, $p = 379$, we have a case of abundant solutions with $M_p = m_p(0) = 5$ and the following residues

exponent j	residues $[\gamma^j]_p$
49	$-147x^5 - 39x^4 - 73x^3 + 138x^2 + 40x + 129$
104	$-169x^5 - 105x^4 - 45x^3 - 180x^2 - 174x + 7$
149	$-91x^5 + 48x^4 - 155x^3 + 62x^2 + 183x + 35$
223	$-178x^5 - 14x^4 - 101x^3 + 150x^2 - 189x + 107$
304	$-103x^5 + 131x^4 + 3x^3 + 165x^2 + 140x + 189$

We have the following examples in the intervals of variations of the 81 values of $\gamma = ax^5 + bx^4 + cx^3 + dx^2 + ex + 1$ (coefficients in $\{-1, 0, 1\}$), of the program for $2000 \leq p \leq 2500$):

a) For $\gamma = x^5 - x^4 - x + 1$ and $p = 2441$, we have $m_p(0) = 2$, $M_p = 6$ (with $u_0 = 1426$) for an exceptional solution (but only for $h = 1$) and the array

exponent j	residues $[\gamma^j]_p$
1	$x^5 - x^4 - x + 1$
915	$-442x^5 - 129x^4 - 125x^3 - 651x^2 - 645x + 376$

For $u_0 = 1426$ we obtain the following array of the residues z giving $M_p = m_p(u_0)$

exponent j	residues $[\gamma^j]_p$
1839	$-169x^5 - 867x^4 - 402x^3 - 891x^2 - 357x - 680$
2034	$35x^5 - 939x^4 - 181x^3 + 388x^2 - 841x - 226$
2054	$449x^5 - 212x^4 + 1097x^3 - 651x^2 + 1191x - 478$
2171	$688x^5 - 525x^4 - 635x^3 + 334x^2 + 181x - 783$
2194	$-909x^5 + 335x^4 - 1136x^3 - 1033x^2 - 970x + 557$
2353	$780x^5 - 1126x^4 + 968x^3 - 264x^2 - 294x - 107$

b) For $\gamma = x^5 - x^4 + x^3 - x^2 + 1$ and $p = 2441$, we have $M_p = m_p(0) = 5$ ($u = 2158, 2057, 724, 359, 0, 717$) for abundant solutions and an analogous array.

c) For $\gamma = x^5 - x^3 - x + 1$ and $p = 2087$, we also have $M_p = m_p(0) = 5$ (with $u = 1335, 950, 670, 1840, 506, 1541, 1102, 280, 1973, 60, 0$) for abundant solutions.

d) Among the 81 generators γ one still find 4 cases of exceptional solutions and 4 cases of distinct abundant solutions.

7.2.6. Conclusions – Fundamental Remarks. Examine the main features of the notions of exceptional and abundant solutions. The number η is fixed and $p \rightarrow \infty$.

(i) *Exceptional solutions.* If $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$, this generates at least h solutions $z_j = \eta^j = [\eta^j]_p \in I_p$, $j = 1, \dots, h$, and this yields $m_p(0) \geq h = O(\log(p))$ (these solutions are also abundant). If we admit that $M_p = O(\log(p))$, we obtain $M_p \geq m_p(0) \geq h$. We shall often have $M_p > m_p(0) \geq h$ taking into account that $M_p = m_p(u_0)$, $u_0 \in [0, p[$, and that $u_0 = 0$ is less probable, even if several u realise M_p ; moreover, $M_p > m_p(0)$, when $u_0 \neq 0$, can be explained by the fact that if $\Delta_p^\theta(z) \equiv u_0 \pmod{p}$, then, in general, $\Delta_p^\theta(\eta^k z) \equiv u_0 \pmod{p}$ (obvious in the

case of linear $\Delta_p^\theta(\bullet)$ in the conjugates of $\alpha_p(\bullet)$; see [Gr2, § 4.2.2 (δ)] for Fermat quotients).

(ii) *Abundant solutions.* If $\Delta_p^\theta(\eta) \not\equiv 0 \pmod{p}$ and $m_p(0) = O(\log(p))$ we then have $O(\log(p))$ solutions $z'_i \in I_p$, $i = 1, \dots, h' := m_p(0)$, where in that case, the solutions z'_i are a priori uniformly distributed in I_p (recall that from [H-B], Fermat quotients are uniformly distributed modulo p and that this property is probably general).

(iii) *Conclusion.* The exceptional case may be seen as the case where, *by accident*, η is part of the solutions z'_j , in which case we have necessarily $z'_1 = \eta$, $z'_2 = \eta^2$, \dots , $z'_h = \eta^h$, with additional z'_i , without one can say that the successive powers of η establish some relations of probabilistic dependence. Moreover, we shall obtain “mixed cases” (i.e., when there exists $\mu \neq \eta$ in I_p , $\mu \ll p$, such that $\Delta_p^\theta(\mu) \equiv 0 \pmod{p}$) giving $h' \ll O(\log(p))$ solutions, in part exceptional).

It follows from all this, that the two cases (i) and (ii) are of similar probabilities, the exceptional case being less probable by definition in which case, only the consideration of the “abondant” case is coherent with the existence of a classical law of probability for the set of solutions z'_i which are not subject to any condition.

In other words, the “exceptional” case would not be particular, despite the appearances, and it would be liable to the same probability as for Fermat quotients ([Gr2, § 4.3.2]), a probability which becomes (for instance) $O(\frac{1}{p^2})$ for $p > p_0$ very large, which we will analyse again.

Remark 7.2. The number η being given, we intend to compare the probability to have a prime number p such that $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$ (exceptional solutions), with the probability to have $\Delta_p^\theta(\eta) \equiv u \pmod{p}$, for fixed u in \mathbb{N} , independently of p (which is the case of $u = 0$). The numerical aspect needs to take u “fixed and small” and to search the prime numbers p such that $\Delta_p^\theta(\eta) \equiv u \pmod{p}$. It is then found the same degree of rarity whatever the choice of u .

For instance if $\eta = x^2 - 3x + 2$ ($x = \zeta_7 + \zeta_7^{-1}$, Pr. B-7 of [Gr4]), in the interval $7 < p \leq 60000001$, we get the rare pairs of solutions

$(p, u) = (61, 0), (5419, 0), (19, 1), (37, 2), (3229, 3), (43, 4), (31, 5), (613, 5), (\emptyset, 6), (79, 7), (42712981, 7)$.

We can use negative u and we get similar results, as $(607, -1), (143137, -1)$.

7.3. On the existence of a binomial law for $m_p(u)$. Besides the previous justifications, we can complete the analysis in the following quantitative manner which results from a very simple computation, given for the case of Fermat quotients $q_p(z)$, $z \in [1, p[$, as well as for the case of local regulators $\Delta_p^\theta(z)$, $z \in I_p$, for the group D_6 and θ of degree 2 (Pr. B-8, B-12, B-13 of [Gr4], the last program testing more general probabilities).

In the two cases, we have computed the mean (under a great lot of prime numbers) the proportions C/N , where for p fixed, C is the number of values $u \in [0, p[$ such that there exists at least a $z \in [2, p-1[$ (resp. $z \in I_p$) such that $q_p(z) \equiv u \pmod{p}$ (resp. $\Delta_p^\theta(z) \equiv u \pmod{p}$).

The very remarkable approximation of the result with $1 - e^{-1} \approx 0.632120$ leads to the following conjecture/heuristic:

Conjecture 7.3. *Let K/\mathbb{Q} be Galois of degree n and of Galois group G . We assume to study the case $f = \delta = 1$ (i.e., p totally split in the field C of values of $\varphi \mid \theta$, $\mathcal{L}^\theta \simeq V_\theta$, cf. Definition 4.1) for p and for the irreducible p -adic character θ . Then the mean value of the proportion of $u \in [0, p[$ of the form $\Delta_p^\theta(z) \pmod{p}$, $z \in I_p$ (Definition 6.1), is equal to $1 - e^{-1} \approx 0.632120$, for $p \rightarrow \infty$.*

The program for C_3 gives the value 0.632133 and that for D_6 gives 0.631711. As we recall at the point (iv) below, it is also the probability (assuming a binomial law) of the existence of at least one solution $z \in I_p$ to $\Delta_p^\theta(z) \equiv u \pmod{p}$ for fixed u .

Then in a complement (unpublished, accessible via [Gr5]), we have estimated, in various manner, the mean value of M_p for the binomial law of probability with parameters $\left(p - 1, \frac{1}{p}\right)$, when $p \rightarrow \infty$ (we ignore if any theoretical result is known).

7.3.1. Second principal heuristic. The previous arguments suggest the existence of a binomial law with parameters $\left(p - 1, \frac{1}{p}\right)$, because we can consider that we realise the $p - 1$ “random selection” $z \in I_p$ for which we ask how many times we get the event $\Delta_p^\theta(z) \equiv u \pmod{p}$, $u \in [0, p[$ given. The second parameter $\frac{1}{p}$ is an approximation of $\text{Prob}(\Delta_p^\theta(z) \equiv u \pmod{p})$.

In fact one can verify that any minor modification of these parameters does not change the conclusion.

Heuristic 7.4. *Let K/\mathbb{Q} be Galois, of degree n and of Galois group G . We assume to study the case $f = \delta = 1$ (cf. Definition 4.1) for p and for the irreducible p -adic character θ of G . Let I_p as defined in Definition 6.1.*

Let $u \in [0, p[$ be fixed. Let $m \in [0, p[$, $m \ll p$; then the probability to have at least m values $z_1, \dots, z_m \in I_p$ such that $\Delta_p^\theta(z_j) \equiv u \pmod{p}$ for $j = 1, \dots, m$, is given by the expression

$$\text{Prob}(m_p(u) \geq m) = \frac{1}{p^{p-1}} \sum_{j=m}^{p-1} \binom{p-1}{j} (p-1)^{p-1-j}.$$

We resend to [Gr2, § 4.4] for identical calculations leading to the following facts, from the simpler formula

$$\text{Prob}(m_p(u) \geq m) = 1 - \left(1 - \frac{1}{p}\right)^p \frac{p}{p-1} \sum_{j=0}^{m-1} \frac{1}{(p-1)^j} \times \binom{p-1}{j},$$

$$(i) \quad \frac{1}{p^{p-1}} \sum_{j=m}^{p-1} \binom{p-1}{j} (p-1)^{p-1-j} < \frac{1}{p^m} \binom{p-1}{m} \text{ for all } m \leq p-1.$$

$$(ii) \quad \text{Prob}(m_p(u) \geq m) \approx 1 - 0.3678 \times \sum_{j=0}^{m-1} \frac{1}{(p-1)^j} \times \binom{p-1}{j}.$$

(iii) The probability to have 0 solutions is near from $e^{-1} \approx 0.3678$.

(iv) The probability to have at least one solution is near from $1 - e^{-1} \approx 0.63212$; for at least 3 (resp. 4) solutions, we obtain 0.0803 (resp. 0.0189).

For an experimental confirmation, see the Pr. 14 of [Gr4].

In the context of minimal p -divisibility, we obtain the following results, where

$$h = \frac{\log(p-1) - \log(2\Gamma(K))}{\log(c_0(\eta))},$$

with $c_0(\eta) = \max_{\sigma \in G}(|\eta^\sigma|)$ (Lemma 6.5):

Lemma 7.5. (i) We have for $p \rightarrow \infty$ the inequalities ([Gr2, Lemma 4.6])

$$\exp\left(-1 + \frac{1}{p}\left(h + \frac{1}{2}\right)\right) < \frac{\frac{1}{p^{p-1}} \cdot \sum_{j=h}^{p-1} \binom{p-1}{j} (p-1)^{p-1-j}}{\frac{1}{p^h} \cdot \binom{p-1}{h}} \leq 1.$$

(ii) It follows $\text{Prob}(\Delta_p^\theta(\eta) \equiv 0 \pmod{p}) < C_\infty(\eta) \times \frac{1}{p^h} \binom{p-1}{h}$ for $p \rightarrow \infty$, where $C_\infty(\eta)$ is between $e^{-1} \approx 0.36788$ and 1.

Lemma 7.6. The series $\sum_{p>2} \frac{1}{p^h} \cdot \binom{p-1}{h}$ is convergent ([Gr2, Lemma 4.7]).

So we obtain the Theorem 1.1 which is modified, compared with the case of Fermat quotient, only by the effective constant $c_0(\eta)$ and the term $O(1)$ which can be precised.

8. p -ADIC CONJECTURES

8.1. Introduction. The previous general result leads to several consequences, or interpretations, that we shall call *Conjectures* insofar as we consider that, under the second principal Heuristic 7.4, any situation leads to the application of the Borell–Cantelli principle. These conjectures come from the suitable use of a p -adic regulator of an $\eta \in K^\times$ and of its θ -components, for $p \rightarrow \infty$, knowing that it is always possible to suppose $\eta \in Z_K$ for the Archimedean aspects of the probabilistic reasoning ($\theta \neq 1$, cf. Lemma 3.8).

In algebraic number theory one speaks of “for almost all prime number p ” to mean “all prime number p except a finite set Σ ”. But other weaker definitions are possible in the probabilistic number theory (cf. [T, Chap. III.3.1]). The statements of this section will be given under the strong form (algebraic).

Whatever the exactness or not of our heuristics, these conjectures are given independently and many seem to be very natural and credible.

8.2. Local interpretation of $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$. Let $\eta \in K^\times$ be such that the multiplicative $\mathbb{Z}[G]$ -module F generated by η is of \mathbb{Z} -rank n and let θ be an irreducible p -adic character of G such that $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$. From the Corollary 3.10 to Theorem 3.9, this is equivalent to the existence of a non trivial θ -relation $U_\theta := \sum_{\nu \in G} u(\nu) \nu^{-1} \in \mathcal{L}^\theta$ such that $\eta^{U_\theta} \in \prod_{v|p} K_v^{\times p}$.

We shall consider this writing as a property of “partial local p th power at p ” of η , according to the following definition:

Definition 8.1. Let $\eta \in K^\times$. We assume that the multiplicative $\mathbb{Z}[G]$ -module F generated by η is of \mathbb{Z} -rank n . Let p be a large enough prime number and let

$$F_{(p)} := \left\{ \eta_0 \in F, \eta_0 \in \prod_{v|p} K_v^{\times p} \right\}.$$

We shall say that η is a *partial local p th power at p* if $\dim_{\mathbb{F}_p}(F/F_{(p)}) < n$.

In the context of this definition, we have the exact sequence

$$0 \longrightarrow \mathcal{L}(\eta) \longrightarrow \mathbb{F}_p[G] \longrightarrow F/F_{(p)} \rightarrow 1,$$

obtained by associating with $U \in \mathbb{F}_p[G]$ the element $\eta^{(p^n p - 1) \cdot U'}$ modulo $F_{(p)}$ where U' is any representative of U in $\mathbb{Z}[G]$.

Remarks 8.2. Since by assumption F is of \mathbb{Z} -rank n and without p -torsion (for all p large enough), we have $F/F^p \simeq \mathbb{F}_p[G]$; in particular

$$\dim_{\mathbb{F}_p}(F/F^p)^{e_\theta} = f \varphi(1)^2,$$

for all θ , where f is the residue degree of θ , cf. § 2.2.4 (ii). This yields the following:

(i) The condition $\dim_{\mathbb{F}_p}(F/F_{(p)}) < n$ is equivalent to the existence of a non trivial θ -relation $U_\theta \in e_\theta \mathbb{Z}_{(p)}[G]$ modulo p , such that η^{U_θ} is in $F_{(p)}$ and not a global p th power in K^\times because $F \cap K^{\times p} = F^p$ for p large enough. Indeed, we have $F \subseteq E^S$ (group of S -units) where S is a suitable finite set of prime ideals of K . If we suppose p large enough such that p does not divide the orders of the torsion groups $\text{tor}_{\mathbb{Z}}(E^S)$ and $\text{tor}_{\mathbb{Z}}(E^S/F)$, then F is a direct facteur in E^S and $E^S = F \oplus H$; if $\eta' \in F$ is such that $\eta' = x^p$, $x \in K^\times$, then $x \in E^S$ and it may be written $x = x_F \times x_H$, whence $x_H^p = 1$, $x_H = 1$ and $\eta' = x_F^p \in F^p$.

(ii) We have

$$(F/F_{(p)})^{e_\theta} \simeq e_\theta \mathbb{F}_p[G]/\mathcal{L}^\theta \simeq \mathbb{F}_p^{(\varphi(1)-\delta) \cdot f \cdot \varphi(1)},$$

since the dimension is $t f \varphi(1)$, $0 \leq t \leq \varphi(1)$, which leads to the relation $t = \varphi(1) - \delta$ since $\mathcal{L}^\theta \simeq \delta V_\theta$ is of \mathbb{F}_p -dimension $\delta f \varphi(1)$.

(iii) To say that $\eta \in F_{(p)}$, is to say that $F_{(p)} = F$, hence $\mathcal{L} = \mathbb{F}_p[G]$, of probability $\frac{O(1)}{p^n}$, a case to be ignored for $n > 1$ and $p \rightarrow \infty$.

In the forthcoming Sections 8.3 and 8.4 we shall look at the reciprocal aspect of these local p th power properties for almost p .

8.3. Case of the characters of order 1 or 2. We return to known particular cases (see § 2.3.3).

8.3.1. Case of a rational. We consider $K = \mathbb{Q}$ with a rational $a \in \mathbb{Q}^\times$, $a \neq \pm 1$. If p is an odd prime number prime to a , we have the elementary following result which is a particular case of the above (for $\theta = 1$ and $U_\theta = 1$):

Lemma 8.3. *The Fermat quotient $\frac{a^{p-1} - 1}{p}$ of a is zero modulo p if and only if $a \in \mathbb{Q}_p^{\times p}$.*

But we know, from a result of Silverman [Si] when $a \in \mathbb{N}$, $a \geq 2$, that under the *ABC* conjecture the set of primes p such that $a^{p-1} \not\equiv 1 \pmod{p^2}$ is infinite.³

The statistical study shows that this result is a very weak form of the reality. In other words, we have the following very reasonable conjectural property:

Conjecture 8.4. *Let $a \in \mathbb{Q}^\times$; if $a \in \mathbb{Q}_p^{\times p}$ for all prime p except a finite number then $a = \pm 1$.*

We may consider this statement as a very particular local-global principle in comparison to those existing in class field theory (then purely algebraic as the “Hasse principle” for powers, recalled in Proposition 8.6).

We might call it a *Diophantine local-global principle* in the perspective that “ $a \in \mathbb{Q}_p^{\times p}$ for almost all p ” would be equivalent to “ $a \in \mathbb{Q}^{\times p}$ for almost all p ”.

³ Silverman proves that for all integer $a \geq 2$, the set of these prime numbers $p \leq x$ is of cardinal $\geq c \log(x)$. This result has been extended by Graves and Murty in [GM] to the $p \equiv 1 \pmod{k}$, for all fixed $k \geq 2$, in which case, the set of these $p \leq x$ is of cardinal $\geq c \frac{\log(x)}{\log(\log(x))}$, still under the *ABC* conjecture.

8.3.2. *Case of a unit of a quadratic field* $K = \mathbb{Q}(\sqrt{m})$. If $\eta = x + y\sqrt{m}$, we have $\eta^{p^{n_p}-1} = 1 + p\alpha_p(\eta)$, $\alpha_p(\eta) = u + v\sqrt{m}$, whence $\Delta_p^\theta(\eta) \equiv 2v\sqrt{m} \pmod{p}$ for $\theta \neq 1$. Thus $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$ if and only if $v \equiv 0 \pmod{p}$.

Suppose $m > 0$ and that η is a unit ε of $\mathbb{Q}(\sqrt{m})$; we have $u \equiv 0 \pmod{p}$ and still $\Delta_p^\theta(\varepsilon) \equiv 2v\sqrt{m} \pmod{p}$; the nullity modulo p of $\Delta_p^\theta(\varepsilon)$ implies $\alpha_p(\eta) \equiv 0 \pmod{p}$, and ε is a local p th power. In a conjectural viewpoint, we are reduced to the previous situation of a rational. Thus it would be sufficient to prove (via a suitable form of the *ABC* conjecture) that the relation $\varepsilon^{p^{n_p}-1} \not\equiv 1 \pmod{p^2}$ occurs for infinitely many p , to be able to state the analogue for ε of the Conjecture 8.4, then the fact that if $\varepsilon^{p^{n_p}-1} \equiv 1 \pmod{p^2}$ for almost all p , then $\varepsilon = \pm 1$.

8.4. Generalization for the degree n . We may suppose that the above process is valuable for the general case where $\eta \in K^\times$ is arbitrary and would be “partial local p th power at p ” (Definition 8.1) for almost all p . This supposes first the analysis of the local p th power case in the usual sense.

8.4.1. *Conjecture about the local p th powers.* The rational case (Conjecture 8.4) showed the reasonableness of the following kind of statements corresponding to the writing $\eta^{p^{n_p}-1} - 1 = p\alpha_p(\eta)$, in the case (statistiquement très exceptionnelle) where $\alpha_p(\eta) \equiv 0 \pmod{p}$, equivalent to $\mathcal{L} = \mathbb{F}_p[G]$ of probability $\frac{O(1)}{p^n}$ (Remark 8.2 and § 4.2.2).

Conjecture 8.5. *Let K be any number field and let $\eta \in K^\times$. If $\eta \in \prod_{v|p} K_v^{\times p}$ for all prime number p except a finite number, then η is a root of unity of K .*

This could result from a generalization of the theorem of Silverman, using here the *ABC* conjecture for the number fields (see for instance the paper of Waldschmidt [W] giving an important list of applications and consequences). But the conjecture can be formulated independently.

This statement is to be compared with the very classical “Hasse principle” for powers, much stronger, and which is the following (cf. e.g. [Gr1, II.6.3.3]):

Proposition 8.6. *Let \mathcal{P}_K (resp. \mathcal{P}_p) be the set of places (resp. of p -places) of K . Let $\eta \in K^\times$ and let p be a prime number; let Σ be a finite set of places of K .*

- (i) *If η is a local p th power for all place $v \in \mathcal{P}_K \setminus \Sigma$, then $\eta \in K^{\times p}$.*
- (ii) *There exist infinitely many (non effective) sets T of places of K such that if η is a local p th power for all place $v \in T$, then $\eta \in K^{\times p}$.⁴*

The difference, regarding the Hasse principle, operates in two times: starting from p and the set \mathcal{P}_p , we begin to say, in the Conjecture 8.5, that η is a local p th power for all $v \in \mathcal{P}_p$ (i.e., we take the infinite set $\Sigma = \mathcal{P}_K \setminus \mathcal{P}_p$; or else we can say that we try to take $T = \mathcal{P}_p$), but after we suppose that this local property (a

⁴The classical statements always suppose that Σ is finite (to eliminate some pathological places) in order to use the density theorem (Chebotarev) which is expressed by means of particular progressions having canonical densities; but to be certain that some of these progressions (finite in number), necessary for the proof, meet the complementary of Σ , this one must be “almost all”, because as soon as an (unknown) infinite family would be missing, it could be that “by accident” it contains the Frobenius that we need. We see the difference that may occur between a general algebraic reasoning and a reasoning on significantly less strong assumptions involving for instance sets Σ of zero density (§ 8.1).

kind of “weaker Hasse principle”) is true for almost all p , in which case η would be conjecturally in $K^{\times p}$ for almost all p (Diophantine local-global principle), hence a root of unity.

The “ultimate” conjecture giving a link with the theories of the $\Delta_p^\theta(\eta)$ is Conjecture 8.9 of § 8.5. Before, let us examine the general case of units of number fields which confirms the previous analysis..

8.4.2. Particular case of the group of units – Spiegelungssatz. We have the following specific statement (cf. e.g. [Gr1, II.6.3.8]).

Proposition 8.7. *Let η be a unit of K and let p be a prime number; let S_p be a finite set of places of K such that the p -class group of $K' := K(\mu_p)$ be generated by the p -classes of the prime ideals $\mathfrak{P}_{v'}$ of K' for the places v' of K' above S_p .*

If $\eta \in K_v^{\times p}$ for all place $v \in S_p \cup \mathcal{P}_p$, then $\eta \in K^{\times p}$.

The Conjecture 8.5 only concerns the set \mathcal{P}_p instead of $S_p \cup \mathcal{P}_p$ for a well-chosen finite set S_p (not sufficient to have a globale p th power), but we assume, in the conjecture, that this weaker hypothesis is true for almost all p . The two systems of assumptions coincide when the p -class group of the field K' is trivial ($S_p = \emptyset$), but we can be more precise (cf. [Gr1, I.6.3.1 and II.1.6.3]).

Let η be a Minkowski unit of a totally real field K ; we can always choose η non global ℓ th power for all prime ℓ . If there exists a θ -relation $U_\theta \not\equiv 0 \pmod{p\mathbb{Z}_{(p)}[G]}$ for which $\eta^{U_\theta} \in \prod_{v|p} K_v^{\times p}$ (i.e. $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$, cf. § 8.2) then the extension

$N' := K'(\sqrt[p]{\eta^{U_\theta}})$ of K' is unramified and p -split which leads, by class field theory, to the following information: let $\mathcal{C}_{K'}^{\mathcal{P}'_p}$ be the quotient of the p -class group $\mathcal{C}_{K'}$ by the p -subgroup of classes of prime ideals $\mathfrak{P}'|p$ in K' and let $\theta^* := \omega\theta^{-1}$, where ω is the p -adic Teichmüller character defined from a primitive p th root of unity ζ_p by

$$\zeta_p^s = \zeta_p^{\omega(s)} \quad \text{for all } s \in \text{Gal}(K'/K).$$

Then it is the θ^* -component of $\mathcal{C}_{K'}^{\mathcal{P}'_p}$ which is non trivial and $\text{Gal}(N'/K')$ is isomorphic to a quotient of $\left(\mathcal{C}_{K'}^{\mathcal{P}'_p}\right)^{e_{\theta^*}}$. This is equivalent to the existence of a p -split θ^* -extension N' of K' , of degree a power of p , contained in $K'(\sqrt[p]{F})/K'$, where F (independent of p) is the G -module generated by η . Such a situation for infinitely many p seems excessive.

Apart from the case of units we have another situation: take for $K = \mathbb{Q}$ the example of $\eta = a \in \mathbb{Q}^\times$, $a \neq \pm 1$. Then the Proposition 8.7 is no longer valid because it only applies if the ideal ηZ_K is the p th power of an ideal, but if $a^{p-1} \equiv 1 \pmod{p^2}$ the extension $\mathbb{Q}(\sqrt[p]{a})/\mathbb{Q}'$ is unramified at p (and p -split) but ramified at the places of \mathbb{Q}' dividing a ; if T is the set of prime divisors of a , we must replace the p -Hilbert class field H' of \mathbb{Q}' by its generalization $H'^{T'}$, the maximal Abelian p -extension unramified outside the places of the set T' above T .

This p -extension $H'^{T'}/\mathbb{Q}'$ is finite because T does not contain p (it is essentially a p -ray class field $K'_{\mathfrak{m}'}$, \mathfrak{m}' built on T') and it plays a role analogous to that of H' ; here we shall have $\theta^* = 1^* = \omega$ and a similar analysis.

8.5. Conjectures on the p -adic regulators $\text{Reg}_p^G(\eta)$. The results of § 8.2 invite to propose the following conjectures stronger than the conjectures of §§ 8.3, 8.4.

Conjecture 8.8. *Let K/\mathbb{Q} be a Galois extension of degree n , of Galois group G . Let $\eta \in K^\times$ be such that the multiplicative $\mathbb{Z}[G]$ -module F generated by η is of \mathbb{Z} -rank n . Then for all p large enough, η is not a partial local p th power at p , in other words, we have $\left\{ \eta_0 \in F, \eta_0 \in \prod_{v|p} K_v^{\times p} \right\} = F^p$, equivalent to $\mathcal{L}(\eta) = \{0\}$.*

The following statement is in fact equivalent to the previous one. Recall that for all irreducible p -adic character θ of G , we have $\text{Reg}_p^\theta(\eta) \equiv \Delta_p^\theta(\eta) \pmod{p}$ and that

$$\text{Reg}_p^G(\eta) := p^{-n} \det(\log_p(\eta^{\tau\sigma}))_{\sigma, \tau \in G}$$

(the normalized p -adic regulator of η , cf. Definitions 2.3 (i)) is factorized into

$$\text{Reg}_p^G(\eta) = \prod_{\theta} \text{Reg}_p^\theta(\eta)^{\varphi(1)} \quad (\text{Remark 2.10}).$$

Conjecture 8.9. *Let K/\mathbb{Q} be a Galois extension of degree n , of Galois group G . Let $\eta \in K^\times$ be such that the multiplicative $\mathbb{Z}[G]$ -module generated by η is of \mathbb{Z} -rank n , and let $\text{Reg}_p^G(\eta)$ the normalized p -adic regulator of η . Then for all p large enough, $\text{Reg}_p^G(\eta)$ is a p -adic unit.*

Remark 8.10. The Conjecture 8.9 implies the Leopoldt–Jaulent conjecture [J] for all prime p except a finite number, but it is preferable to admit this last one, very classical, and to say that the Conjecture 8.9 is a stronger version (cf. § 2.1.4, (a) and (b)). By negation, we get that if there exist infinitely many primes p such that $\text{Reg}_p^G(\eta) \equiv 0 \pmod{p}$, then the \mathbb{Z} -rank of the $\mathbb{Z}[G]$ -module generated by η is $< n$.

8.6. Conjectures about the Abelian p -ramification for real fields. Let H^{pr} be the maximale Abelian p -ramified (i.e., unramified outside p) p -extension of a real Galois number field K satisfying the Leopoldt conjecture for all p . Let \hat{K} be the cyclotomic \mathbb{Z}_p -extension of K and let $\mathcal{T}_p = \text{Gal}(H^{pr}/\hat{K})$. For all p large enough, $|\mathcal{T}_p|$ has the same p -adic valuation as the normalized regulator of K

$$p^{1-n} \mathcal{R}_p(K) \sim \prod_{\theta \neq 1} \text{Reg}_p^\theta(\varepsilon)^{\varphi(1)},$$

where ε is a fixed suitable Minkowski unit of K ([Coa], [Gr1, III.2.6.5]).

The Conjecture 8.9 implies the following conjecture that we may state for a non necessary Galois (nor real) field because if K is any Galois field and \mathcal{T}_p the torsion subgroup of the Galois group $\text{Gal}(H^{pr}/\hat{K})$, where \hat{K} is the compositum of the \mathbb{Z}_p -extensions of K , for $K' \subseteq K$, $\mathcal{T}_p(K')$ is isomorphic to a subgroup of $\mathcal{T}_p(K)$ under the Leopoldt conjecture ([Gr1, IV, §2]), and any component \mathcal{T}_p^θ , θ odd, is trivial for all p large enough since it depends on the θ -component of the p -class group of K ([Gr1, III.2.6.1, Fig. 2.2]):

Conjecture 8.11. *The invariant $\prod_p \mathcal{T}_p$ is finite, for all number field satisfying the Leopoldt conjecture for all p .*

Remarks 8.12. (i) Recall that an arbitrary field K , such that $\mathcal{T}_p = 1$ under the Leopoldt conjecture, is said to be p -rational and that in this case the arithmetic of K becomes essentially trivial (see a synthesis of the properties in [Gr1, IV.3 (b)], [MN], and the links with the p -regularity whose beginnings are in [Gr3] then [JN], among an abundant subsequent bibliography on the subject recalled in [Gr7]).

For K real and for all $p \geq 2$, the p -rationality implies easily the Greenberg conjecture ([Gre], [Gr8]), which clarifies the context.

(ii) We shall deduce, from the above, analogous properties on the residue of the p -adic zêta function ([Coa, Appendix], and [Se2]). When the p -valuation of $\zeta_K(2-p)$ is negative, it is equal to -1 ([Se2, Théorème 6]); in the context of Conjecture 8.11, we would have $\frac{\zeta_K(2-p)}{\zeta_{\mathbb{Q}}(2-p)} \sim |\mathcal{T}_p| = 1$ for all p large enough ([Hat]).

(iii) Let S be the set consisting of the p -places of K and infinite places, and let $G_S(K)$ be the Galois group of the maximal S -ramified (i.e., unramified outside S) algebraic extension of K ; then in a cohomological point of view, we would have the duality $H^2(G_S(K), \mathbb{Z}_p) \simeq \mathcal{T}_p^* = 1$, for all p large enough.

8.7. More general cohomological justifications. We give here some comments about results whose mathematical level largely exceeds any heuristic approach, but this confrontation has seemed to us very convincing. We may refer to several papers in [BK] of which [Ko] and [Ng].

The main central idea, related to the conjecture of Bloch–Kato, is that there exists, in a rather systematic way, global *finite* invariants whose p -adic specializations, of a cohomological nature, are the arithmetical objects (more or less classical) of a number field K (as the p -class groups, the groups \mathcal{T}_p of p -ramification, some p -adic regulators, certain étale cohomological groups, ...). This conjectural point of view is universally admitted, all the more that some proofs have been given quite extensively. Let us recall briefly the main known results:

We start from the notation of § 8.6. For $m \in \mathbb{Z}$, let $\mathbb{Z}_p(m)$ be the $G_S(K)$ -module \mathbb{Z}_p provided with the action defined by the character χ^m , where $\chi : G_S(K) \rightarrow \mathbb{Z}_p^\times$ is the character of the action of $G_S(K)$ on μ_{p^∞} .

We say that K is (p, m) -rational if $H^2(G_S(K), \mathbb{Z}_p(m))$ is trivial; the usual p -rationality mentioned § 8.6 corresponds to $m = 0$ which seems to be the most delicate case. The finiteness of $H^2(G_S(K), \mathbb{Z}_p(m))$ is equivalent to a m -analogue of the Leopoldt conjecture in terms of “suitable p -adic regulators”.

The results on the finiteness of some global objects whose p -adic specializations are the $H^2(G_S(K), \mathbb{Z}_p(m))$, for m fixed, are the following ones (from private indications by Thong Nguyen Quang Do):

(i) For $m \geq 2$, this is a consequence of the “Quillen–Lichtenbaum conjecture” now Voevodsky Theorem. The finiteness comes from that of the K-theory groups $K_{2m-2}(Z_K)$ via a non trivial isomorphism of the following form ($p > 2$)

$$K_{2m-2}(Z_K) \otimes \mathbb{Z}_p \simeq H^2(G_S(K), \mathbb{Z}_p(m)).$$

(ii) The case $m = 1$ corresponds, under a similar form (due to the fact that the cohomology group is not finite because of the Brauer group), to the Gross conjecture, and the case $m < 0$ is essentially unknown: if $m < 0$ is odd, then $H^2(G_S(K), \mathbb{Z}_p(m))$ is finite; the case $m < 0$ even is unknown.

(iii) The case $m = 0$ defines the framework “Leopoldt conjecture and torsion p -group \mathcal{T}_p , dual of $H^2(G_S(K), \mathbb{Z}_p)$ ”, a framework in which a similar situation is conjectured, in the line of the previous “motivic work” of Voevodsky.

Thus our conjectural Diophantine approach is enforced by the deep results recalled above, the interest being that the notion of (normalized) p -adic regulator of an arbitrary algebraic number is more general.

9. CONCLUSION

We have tried to give a maximum of justifications, in particular by the fact that when the probabilities of p -divisibility of $\text{Reg}_p^G(\eta)$ are at most $\frac{O(1)}{p^2}$, the heuristic principle of Borel–Cantelli suggests a finite number of solutions p and even no solution most of the time since the sum of the $\frac{1}{p^2}$ is very small

$$\sum_{p \geq 2} \frac{1}{p^2} \approx 0.45, \quad \sum_{p \geq 10^4} \frac{1}{p^2} \approx 9 \times 10^{-6}.$$

It remains the case of minimal p -divisibility $\text{Reg}_p^G(\eta) \sim p^{\varphi(1)}$ (Definition 4.1) which is a possible obstruction if the Heuristic 7.4 is inaccurate; in that case, the “expected number of solutions” $p \leq x$ would be $O(1)\log_2(x) + O(1)$ and the corresponding arithmetical p -adic invariants (seen in §8.7) would have, for all p large enough, a minimal canonical structure of G -module (e.g. $H^2(G_S(K), \mathbb{Z}_p) \simeq V_\theta$ for a unique θ such that $f = \delta = 1$).

It would be useful to have an analytical estimation of M_p which precises the notions of exceptional and abundant solutions (cf. §7.1; see also [Gr5]).

But if there is some consistency of mathematics, then we can believe that such conjectures of finiteness are legitimate.

For instance, we can deduce from this study that the Leopoldt–Jaulent conjecture on the non nullity of the p -adic regulators is an extremely weak form of the reality.

Acknowledgments. I would like to thank Ján Mináč for his friendly support about this article, Thong Nguyen Quang Do for his “cohomological” comments, and Gérald Tenenbaum for useful information on probabilistic number theory. Finally I warmly thank the anonymous Referee for his careful reading and remarks.

REFERENCES

- [BK] J. Coates, A. Raghuram, A. Saikia, R. Sujatha (Eds), *The Bloch–Kato Conjecture for the Riemann Zeta Function*, Conf. July 2012, London Math. Soc. Lecture Note Series (2015).
- [CDP] R. Crandall, K. Dilcher, and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. 66, 217 (1997), 433–449. <https://math.dartmouth.edu/~carlp/PDF/paper111>
- [Coa] J. Coates, *p -adic L -functions and Iwasawa’s theory*, In: Proc. of Durham Symposium 1975, New York-London (1977), 269–353.
- [C] K. Conrad, The origin of representation theory, Enseign. Math. 44 (1998), 361–392. <http://www.math.uconn.edu/~kconrad/articles/groupdet>
- [EM] R. Ernvall and T. Metsänkylä, On the p -divisibility of Fermat quotients, Math. Comp. 66 (1997), 1353–1365. <http://www.ams.org/journals/mcom/1997-66-219/S0025-5718-97-00843-0/>
- [GM] H. Graves and M.R. Murty, *The abc conjecture and non-Wieferich primes in arithmetic progressions*, Journal of Number Theory 133 (2013), 1809–1813. <http://www.sciencedirect.com/science/article/pii/S0022314X12003368>
- [Gr1] G. Gras, *Class Field Theory: from theory to practice*, SMM, Springer-Verlag 2003; second corrected printing 2005. <https://www.researchgate.net/publication/268005797>
- [Gr2] G. Gras, *Étude probabiliste des quotients de Fermat*, Functiones et Approximatio, Commentarii Mathematici, Vol. 54, 1 (2016). <http://projecteuclid.org/euclid.facm/1458656166>
- [Gr3] G. Gras, *Remarks on K_2 of number fields*, Jour. Number Theory 23 (1986), 322–335.
- [Gr4] G. Gras, *Conjectures p -adiques – Programmes PARI*, <https://www.researchgate.net/publication/296939717>
- [Gr5] G. Gras, *Compléments heuristiques et probabilistes sur les quotients de Fermat*, <https://www.researchgate.net/publication/301287416>

- [Gr6] G. Gras, *On the order modulo p of an algebraic number*, preprint 2016/2017. <https://www.researchgate.net/publication/282317486>
- [Gr7] G. Gras, *Sur le module de Bertandias-Payan dans une p -extension – Noyau de capitulation*, Publ. Mathématiques de Besançon, Algèbre et Théorie des Nombres(2016), 25–44. <https://www.researchgate.net/publication/294194005>
- [Gr8] G. Gras, *Approche p -adique de la conjecture de Greenberg (cas totalement réel p -décomposé)*, preprint (2016/2017). <https://arxiv.org/pdf/1611.09592.pdf>
- [Gre] R. Greenberg, *Iwasawa theory - past and present*, Class field theory - its centenary and prospect (Tokyo 1998), Adv. Studies in Pure Math., Math. Soc. Japan (2001), 335–385.
- [Hat] K. Hatada, Mod 1 distribution of Fermat and Fibonacci quotients and values of zeta functions at $2 - p$, Comment. Math. Univ. St. Pauli 36 (1987), 41–51.
- [H-B] R. Heath-Brown, *An Estimate For Heilbronn's Exponential Sum*, In: Conference in honor of Heini Halberstam, Analytic Number Theory, 2 (1996), Birkhäuser 1996. <http://eprints.maths.ox.ac.uk/157/1/heilbron.pdf>
- [J] J-F. Jaulent, Sur l'indépendance ℓ -adique de nombres algébriques, Journal of Number Theory 20 (1985), 149–158. <http://www.sciencedirect.com/science/article/pii/0022314X85900356>
- [JN] J-F. Jaulent et T. Nguyen Quang Do, *Corps p -rationnels, corps p -réguliers et ramification restreinte*, J. Théor. Nombres Bordeaux 5 (1993), 343–363. <https://www.researchgate.net/publication/236865222>
- [Ko] M. Kolster, *The Norm Residue Theorem and the Quillen-Lichtenbaum Conjecture*, In: J. Coates, A. Raghuram, A. Saikia, R. Sujatha (Eds), The BlochKato Conjecture for the Riemann Zeta Function, Conf. July 2012, London Math. Soc. Lecture Note Series (2015).
- [KR] W. Keller and J. Richstein, *Solutions of the congruence $a^{p-1} \equiv 1 \pmod{p^r}$* , Math. Comp., 74, 250 (2004), 927–936. <http://www.ams.org/journals/mcom/2005-74-250/S0025-5718-04-01666-7/>
The continuing search for Wieferich primes, Math. Comp., 75, 251 (2005), 1559–1563. <http://www.ams.org/journals/mcom/2005-74-251/S0025-5718-05-01723-0/>
- [MN] A. Movahhedi and T. Nguyen Quang Do, *Sur l'arithmétique des corps de nombres p -rationnels*, Séminaire de Théorie des Nombres, Paris 1987–88, Progress in Mathematics Volume 81, 1990, 155–200.
- [Ng] T. Nguyen Quang Do, *On the Determinantal Approach to the Tamagawa Number Conjecture*, In: J. Coates, A. Raghuram, A. Saikia, R. Sujatha (Eds), The BlochKato Conjecture for the Riemann Zeta Function, Conf. July 2012, London Math. Soc. Lecture Note Series (2015).
- [OS] A. Ostafe and I.E. Shparlinski, *Pseudorandomness and dynamics of Fermat quotients*, SIAM J. Discrete Math. 25, 1 (2011), 50–71. <http://epubs.siam.org/doi/abs/10.1137/100798466>
- [P] K. Belabas and al., *Pari/gp, Version 2.5.3*, Laboratoire A2X, Université de Bordeaux I. <http://sagemath.org/>
- [Se1] J-P. Serre, *Représentations linéaires des groupes finis*, cinquième édition corrigée et augmentée de nouveaux exercices, Coll. Méthodes, Hermann 1998.
- [Se2] J-P. Serre, *Sur le résidu de la fonction zêta p -adique d'un corps de nombres*, C.R. Acad. Sci. Paris 287, Série I (1978), 183–188.
- [Sh] I.E. Shparlinski, *On Vanishing Fermat Quotients and a Bound of the Ihara Sum*, Kodai Math. J. Volume 36, Number 1 (2013), 99–108. <http://projecteuclid.org/euclid.kmj/1364562722>
- [Si] J.H. Silverman, *Wieferich's criterion and the abc-conjecture*, Journal of Number Theory 30 (1988), 226–237. <http://www.sciencedirect.com/science/article/pii/0022314X88900194>
- [T] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, 3^e édition revue et augmentée, Coll. Échelles, Belin 2008.
- [W] M. Waldschmidt, *Lecture on the abc conjecture and some of its consequences*, Abdus Salam School of Mathematical Sciences (ASSMS), Lahore 6th World Conference on 21st Century Mathematics (2013). <http://www.math.jussieu.fr/~miw/articles/pdf/abcLahore2013VI>
- [Wa] L.C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math. 83, Springer enlarged second edition 1997.

VILLA LA GARDETTE, CHEMIN CHÂTEAU GAGNIÈRE, F-38520 LE BOURG D'OISANS.

E-mail address: g.mn.gras@wanadoo.fr url: http://www.researchgate.net/profile/Georges_Gras